тер, для проведения успешного криптоанализа определенной криптосистемы.
Ключевые слова: алгоритм Гровера, блочный симметричный шифр, NTRU, кольца срезанных полиномов, устойчивость.

ANALYSIS OF RESISTANCE POPULAR CRYPTOSYSTEMS AGAINST QUANTUM CRYPTANALYSIS BASED ON GROVER'S ALGORITHM

The problem of resistance the popular cryptosystems against quantum cryptanalysis is an urgent and important task, given the pace of development of quantum technologies. Resistance of all modern cryptosystems based on the complexity of solving certain mathematical problems. Such mathematical problems tend to have exponential complexity or subexponential solutions, using quantum algorithms that have been proposed Shore and Grover the complexity of solving such problems is reduced to a polynomial. So Shor's algorithm reduces the complexity of cryptanalysis transformations in the ring, field and in the group of points on elliptic curves. The article describes the using of Grover's algorithm for cryptanalysis popular symmetric block ciphers. The methods of quantum cryptosystems cryptanalysis NTRU, based on a combination of classical attacks and meeting in the middle of Grover's quantum algorithm. In this paper we proposed our estimates of resistance of block popular ciphers and cryptosystems NTRU with different sizes of the quantum system-wide parameters against cryptanalysis based on the use of Grover's quantum algorithm. The article also shows the characteristics that must have a quantum computer for successful cryptanalysis of certain cryptosystems.
Index Terms: Grover's algorithm, block symmetric cipher, NTRU, the ring of truncated polynomials, stability.

Горбенко Юрій Іванович, кандидат технічних наук, старший науковий співробітник Харківського національного університету радіоелектроніки, лауреат Державної премії в галузі науки та техніки.
E-mail: GorbenkoU@iit.com.ua
Горбенко Юрий Иванович, кандидат технических наук, старший научный сотрудник Харьковского национального университета радиоэлектроники, лауреат Государственной премии в области науки и техники.
Gorbenko Yuriy, Ph.D., senior research fellow of Kharkiv National University of Radio Electronics, Laureate of the State Prize in Science and Technology.

Ганзя Роман Сергійович, аналітик систем захисту інформації ЧАО «ІІТ».
E-mail: roman.ganzya@gmail.com
Ганзя Роман Сергеевич, аналитик систем защиты информации ПрАТ «ИИТ».
Ganzya Roman, analyst of security systems of JSC «IIT».

УДК 511.512

ПРОГРАММНО-МОДЕЛИРУЮЩИЙ КОМПЛЕКС SCSPS АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ

Анатолий Белецкий, Денис Навроцкий, Александр Семенюк

Основу SCSPS алгоритма поточного шифрования образуют шенноновские примитивы нелинейной подстановки (Substitution) и перестановки (Permutation), или так называемые SP-сети, дополненные примитивами «скользящего кодирования» (SlideCode) и стохастического циклического сдвига (Shift). Поточное шифрование осуществляется поразрядным сложением по модулю 2 блоков шифруемого текста, размер которых составляет 128, 192 или 256 бит, с равными по длине блоками двоичных псевдослучайных чисел (ключами, или гаммами). Поток гамм вырабатывается совокупностью криптографических преобразований секретного базового ключа шифрования. Моделирующий комплекс допускает возможность исключения одного или нескольких примитивов из алгоритма шифрования. Проведен анализ эффективности SCSPS алгоритма.
Ключевые слова: *криптографические примитивы, поточные шифры, программно-моделирующий комплекс.*

I. Введение и постановка задачи. В тех случаях, когда шифрование данных необходимо осуществлять в реальном времени, когда требуется высокая скорость передачи информации (например, при трансляции «живого» видео, в системах сотовой связи и др.), или при передаче по каналам связи массивов данных большого объема зачастую применяют поточные шифры [1].

Различают два основных типа поточных шифров: *синхронные* и *асинхронные* шифры. В синхронных поточных шифрах (СПШ) ключевая (шифрующая) псевдослучайная последовательность (ПСП), называемая *гаммой шифра* (или просто гамма), формируется независимо как от входного (шифруемого) текста, так и шифротекста. При таком способе поточного шифрования от-

сутствует эффект размножения ошибок. Это означает, что число искаженных элементов в расшифрованном тексте равно числу искаженных элементов зашифрованной последовательности, принятых по каналу связи. Вместе с тем, вставка или выпадение отдельных элементов зашифрованной последовательности всегда приводит к неправильному расшифрованию всех последующих элементов текста.

В асинхронных поточных шифрах (АПШ), называемых также *самосинхронизирующимися* шифрами, ключевой поток создаётся функцией ключа и фиксированного числа знаков шифротекста, за счет чего АПШ могут оказаться более устойчивыми к атакам, чем СПШ [2].

В качестве элементов последовательности двоичных входных данных, подвергаемых криптографическим преобразованиям в поточных шифрах, выступают, как правило, биты (в таком случае шифры называют *бит-ориентированными* шифрами) или байты (*байт-ориентированные* шифры) и реже элементы, длина которых превышает байт.

Представителем бит-ориентированных поточных шифров является шифр *A5* (и его модификации), используемый для обеспечения конфиденциальности передаваемой по радиоканалу информации в стандарте мобильной сотовой связи GSM [3]. Шифр основан на побитовом сложении по модулю два (булева операция XOR) генерируемой ПСП и шифруемой информации. В качестве байт-ориентированного поточного шифра можно привести шифр RC4 [4], широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколах SSL и TLS [5], алгоритме WEP шифрования и обеспечения безопасности беспроводных Wi-Fi сетей [6]). И, наконец, шифр Rabbit относится к поточным шифрам, посредством которого входной текст преобразуется блоками по 128 бит, перемешивая внутреннее состояние ключа шифрования между двумя последовательными итерациями (блоками шифрования) [7]. Функция перемешивания в шифре Rabbit основана исключительно на линейных арифметических операциях, то есть для реализации криптографических преобразований входного текста в этом шифре не используются операторы нелинейные замены (подстановки).

Основная задача данной статьи состоит в разработке программно-моделирующего комплекса шифра, обеспечивающего скоростное поточное криптографическое преобразование открытого текста последовательностью псевдослучайных гамм, длина которых N составляет 128, 192 или 256 бит. Для ослабления статистической связи между смежными гаммами в предлагаемом алгоритме наряду с операторами линейного перемешивания шифрующих гамм, реализуемых примитивами «скользящего кодирования» SlideCode, перестановки Permutation и стохастического циклического сдвига Shift, применяется также примитив нелинейной замены Substitution байтов этих гамм.

II. Базовый алгоритм SCSPS шифрования. Принцип работы SCSPS шифра поясняется схемой, показанной на рис. 1.

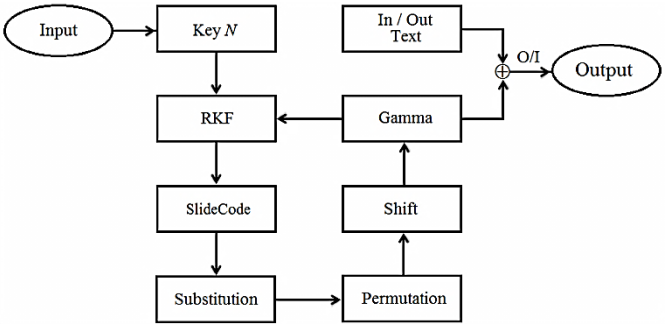


Рис. 1. Структурно-логическая схема SCSPS шифра

На этапе инициализации шифра секретный N – битный ключ (Key) размещается в регистре ключевого поля RKF (Register Key Field). Содержимое регистра циклически обновляется последовательностью преобразований, который включает: примитивы «скользящего кодирования» (SlideCode), нелинейной подстановки в блоке Substitution (S-блоке), линейной перестановки (Permutation) и управляемого стохастического сдвига (Shift). В результате таких преобразований образуется поток гамм, посредством которых осуществляется как зашифрование входного текста (InText), так и расшифрование выходного текста (OutText).

Ниже приведены краткие описания примитивов, участвующих в формировании потока двоичных псевдослучайных последовательностей, которые образуют шифрующие гаммы длины N.

Примитив «скользящего кодирования» (обозначаемый далее на интерфейсах как блок SlideCode) может быть реализован в двух вариантах: одностороннего SC1 или двухстороннего SC2 кодирования. Способ реализации варианта SC1 отображен на рис. 2.

Согласно рис. 2, одностороннее «скользящее кодирование» (СК) представляет собою классическое (левостороннее, т.е. выполняемое по направлению слева направо) обратное преобразование Грея [8], в котором x_k и y_k – биты на входе и выходе примитива СК.

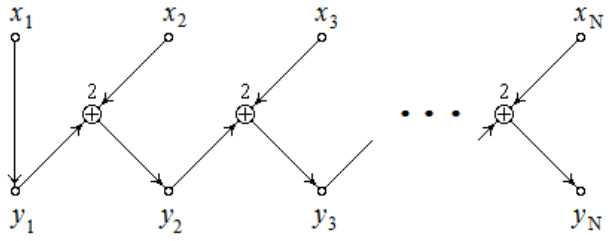


Рис. 2. Левостороннее «скользящее кодирование»

При двустороннем «скользящем кодировании» (вариант SC2) сначала выполняется левостороннее СК (рис. 2), а после этого – правостороннее кодирование, схема которого (рис. 3) совпадает с обратным правосторонним преобразованием Грея [9].

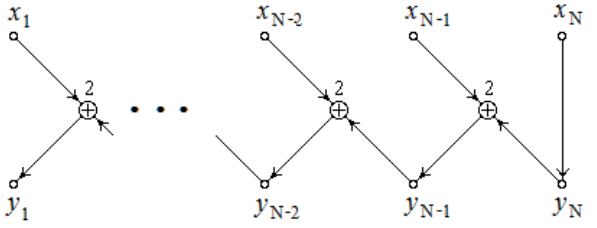


Рис. 3. Правостороннее «скользящее кодирование»

Таким образом, примитив СК есть не что иное, как преобразование Грея «наоборот», т.е. прямое СК выполняется по схеме вычисления обратного кода Грея (КГ). Обратное СК совпадает с прямым КГ, но в шифре SCSPS такое преобразование не применяется.

Примитив нелинейной подстановки Substitution (блок SubByte) выполняет преобразование

$$y = (x+\alpha)_f^{-1} \cdot A_{\omega,\varphi} + \beta, \qquad (1)$$

где x – исходный байт формируемой гаммы, замещаемый байтом y; α и β – восьмибитные аддитивные компоненты преобразования; g_f^{-1} – элемент, мультипликативно обратный элементу g расширенного поля $GF(2^8)$, порождаемого неприводимым полиномом (НП) восьмой степени f; $A_{\omega,\varphi}$ – невырожденная двоичная матрица Галуа восьмого порядка, которая составляется на основании НП φ и образующего элемента ω (алгоритм синтеза матриц Галуа поясняется ниже).

Матричные преобразования в (1) выполняются в кольце вычетов по модулю 2. Соотношение (1) обобщает классическое S-преобразо-вание шифра AES [10], в котором

$$y = x_f^{-1} \cdot A + \gamma, \qquad (2)$$

причем НП $f = 100011011$, аддитивная компонента $\gamma = 01100011$ и A – циркулянтная матрица, верхняя строчка которой равна 10001111. Все последующие (по направлению сверху вниз) строчки матрицы A образуются циклическим сдвигом предшествующих им строк на один разряд вправо.

Матрицы $A_{\omega,\varphi}$ в (1) названы *обобщенными матрицами Галуа* [11] на том основании, поскольку они участвуют в построении генераторов двоичных ПСП на *обобщенных линейных регистрах сдвига* с линейными обратными связями *по схеме Галуа* [12]. Суть алгоритма синтеза обобщенных матриц Галуа $n-$го порядка состоит в следующем. Пусть $\varphi_n -$двоичный НП степени n и $\omega \geq 10 -$ образующий элемент (ОЭ) матрицы, являющийся элементом расширенного поля $GF(2^n)$, порождаемого НП φ_n. ОЭ ω записывается в нижней строке матрицы $A_{\omega,\varphi}$. Элементы строки, расположенные левее ω, заполняются нулями. Последующие строки матрицы (по направлению снизу вверх) образуются обычным сдвигом предыдущей строки на один разряд влево. Если при этом левый элемент сдвигаемой строки равен 1, то разрядность сформированной строки оказывается на единицу больше порядка матрицы. Векторы, отвечающие таким строчкам, приводятся к остатку по модулю НП φ_n и, тем самым, также становятся $n-$разрядными.

Пусть, для примера, $n = 8$, $\varphi_n = 101001101$ и $\omega = 101101$. Воспользовавшись приведенным алгоритмом синтеза, приходим к матрице Галуа, представленной соотношением

$$A_{\omega,\varphi} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Отметим интересное свойство матриц Галуа, синтезируемых выше изложенным способом. Из теории многочленов (полиномов) одной переменной, которую обозначим x, известно, что умножение произвольного полинома $\varphi_n(x)$ степени n на x эквивалентно сдвигу полинома на один разряд влево и, соответственно, увеличению на 1 степени полинома, т.е.

$$x \cdot \varphi_n(x) \to \varphi_{n+1}(x). \qquad (3)$$

Воспользовавшись выражением (3), представим матрицу $A_{\omega,\varphi}$ порядка n в таком виде:

$$A_{\omega,\varphi}=\begin{pmatrix} x^{n-1}\cdot\omega \\ x^{n-2}\cdot\omega \\ \cdots \\ x\cdot\omega \\ \omega \end{pmatrix}(\mathrm{mod}\,\varphi)=\omega\cdot\begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix}(\mathrm{mod}\,\varphi). \quad (4)$$

Запишем каждый моном правого вектор-столбца (4) в двоичной форме и, тем самым, получим

$$\begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}=E_n, \quad (5)$$

где E_n – единичная матрица порядка n.

На основании системы равенств (4) и (5) приходим к представлению

$$A_{\omega,\varphi}\,(\mathrm{mod}\,\varphi)\leftrightarrow\omega,$$

согласно которому матрицы Галуа $A_{\omega,\varphi}$ являются изоморфными образующим их элементам ω и, как следствие, сохраняют свойства этих элементов. Это означает, в частности, что если ω – примитивный элемент поля $GF(2^n)$, порождаемого НП φ степени n, то и $A_{\omega,\varphi}$ также становится *примитивной матрицей*. Двоичная $(n\times n)$ матрица является примитивной, если последовательность степеней этой матрицы образует циклическую группу максимального порядка 2^n-1.

Принципиальное отличие S-блоков SCSPS и AES шифров, заданных выражениями (1) и (2) соответственно, состоит в следующем. Во-первых, S-преобразование (1) содержит аддитивную составляющую α, которая отсутствует в S-блоке AES шифра. И, во-вторых, в отличие от AES шифра с постоянными параметрами f, γ и A в преобразовании (2) все параметры преобразования (1), а именно, компоненты α и β, f, ω, и φ могут быть вариабельными. Общая длина таких параметров составляет порядка 37 бит. Тем самым, если указанные параметры шифра являются секретными, то эффективная длина ключа шифрования возрастает на это же число бит, что приводит к повышению криптостойкости SCSPS алгоритма.

И, наконец, отметим, что примитив Substitution может быть использован в двух режимах: SB1 и SB2. В режиме SB1 осуществляется преобразование байтов модифицируемого ключа шифрования *Key* (гаммы) ранее описанным способом. В режиме SB2 сначала выполняется S-преобразование ключа *Key* по схеме SB1, а затем – аналогичное преобразование столбцов квадратной матрицы восьмого порядка. Строки таких 64-битных матриц как бы заполняются байтами регистра RKF. Реально биты столбцов матриц набираются программным способом из содержимого регистра RKF, исключая физическое формирование самих матриц. Из приведенного пояснения становится, по крайней мере, понятным, что длина ключа *Key* должна быть кратной 64 битам.

Примитив Permutation (блок Permut) осуществляет табличную перестановку элементов формируемой гаммы блоками, длина которых составляет $l=N/r$ бит, где $N-$размер гаммы, а $r-$число элементов, на которое разбивается гамма. В SCSPS шифре $r=8$, 16 или 32. Таблица перестановки содержит r строк, каждая из которых представляет собой стохастическую последовательность чисел из интервала $\overline{0,r-1}$.

Содержимое ячейки формируемой гаммы (ключа шифрования) переносится в ячейку, номер которой указан в строках таблицы. В свою очередь номер строки таблицы выбирается из назначенных разрядов регистра Substitution.

Примитив Shift (блок ShiftRow) выполняет стохастический сдвиг формируемой гаммы. В блоке ShiftRow осуществляется круговая прокрутка содержимого регистра, сохраняющего отклик примитива Permutation, на нечетное число Z. Параметр Z вычисляется следующим образом. Все байты гамм поразрядно суммируются по mod 2 и в младший разряд результирующего байта, обозначим его B, заносится 1 (для обеспечения нечетности сдвига). Если длина гаммы составляет $N=128$ или 192 бит, то значение параметра прокрутки Z задается шестью младшими разрядами байта B. Для $N=256$ бит параметр Z определяется содержимым семи младших разрядов этого байта.

III. Описание моделирующего комплекса. Окна (и клавиши) инициализации основных примитивов и выполняемых функций моделирующего комплекса показаны на рис. 4. Нажатием на клавишу «Генерировать» запускается генератор случайных чисел, которым формируется стартовый ключ *Key* размером 16, 24 или 32 байта, записываемых в 16-ричной форме в нижнем окне интерфейса.

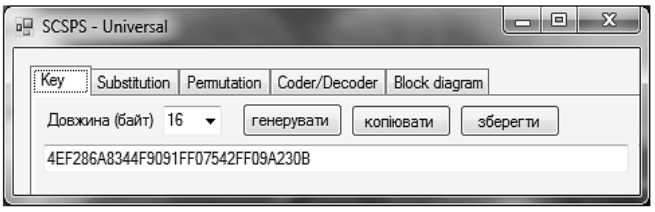


Рис. 4. Базовый интерфейс программно-моделирующего комплекса

Параметризация примитива Substitution (рис. 5) предполагает независимый выбор полиномов f и φ из 30 НП восьмой степени, аддитивных составляющих α и β, а также ОЭ ω матрицы A.

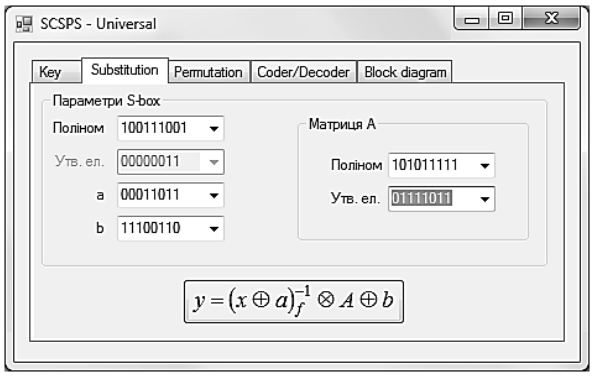
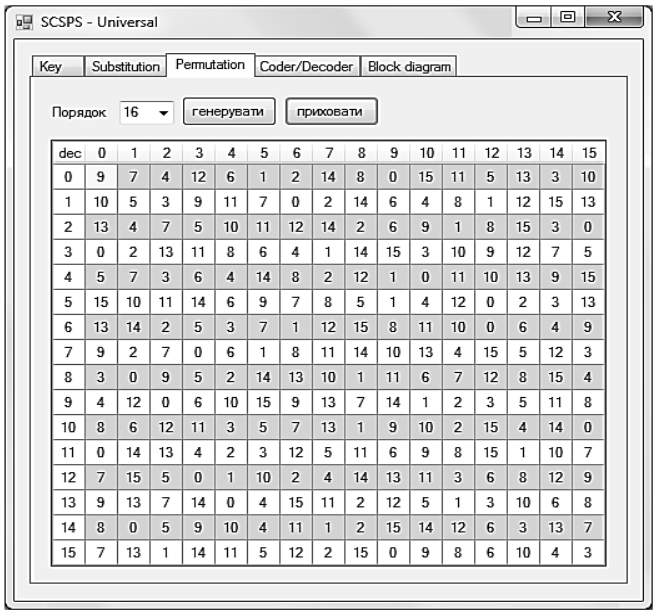


Рис. 5. Интерфейс примитива Substitution

В затененное окно интерфейса (рис. 5) выводится минимальный примитивный элемент поля $GF(2^8)$, порождаемого НП f.

На рис. 6 приведен вариант таблицы перестановок 16 порядка, которая образована на этапе параметризации примитива Permutation.



dec	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	9	7	4	12	6	1	2	14	8	0	15	11	5	13	3	10
1	10	5	3	9	11	7	0	2	14	6	4	8	1	12	15	13
2	13	4	7	5	10	11	12	14	2	6	9	1	8	15	3	0
3	0	2	13	11	8	6	4	1	14	15	3	10	9	12	7	5
4	5	7	3	6	4	14	8	2	12	1	0	11	10	13	9	15
5	15	10	11	14	6	9	7	8	5	1	4	12	0	2	3	13
6	13	14	2	5	3	7	1	12	15	8	11	10	0	6	4	9
7	9	2	7	0	6	1	8	11	14	10	13	4	15	5	12	3
8	3	0	9	5	2	14	13	10	1	11	6	7	12	8	15	4
9	4	12	0	6	10	15	9	13	7	14	1	2	3	5	11	8
10	8	6	12	11	3	5	7	13	1	9	10	2	15	4	14	0
11	0	14	13	4	2	3	12	5	11	6	9	8	15	1	10	7
12	7	15	5	0	1	10	2	4	14	13	11	3	6	8	12	9
13	9	13	7	14	0	4	15	11	2	12	5	1	3	10	6	8
14	8	0	5	9	10	4	11	1	2	15	14	12	6	3	13	7
15	7	13	1	14	11	5	12	2	15	0	9	8	6	10	4	3

Рис. 6. Интерфейс примитива Permutation

Интерфейс шифрования (рис. 7), открывается клавишей Coder/Decoder.

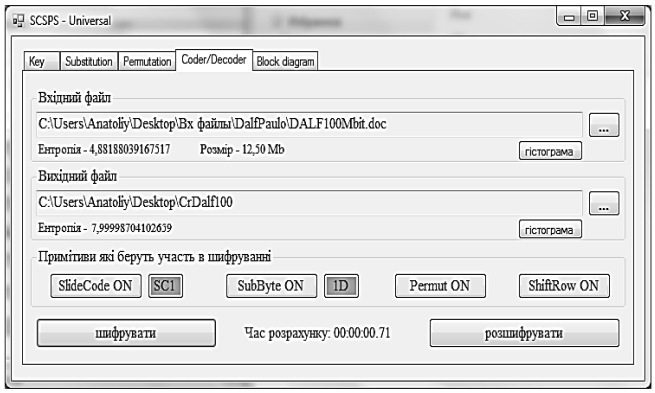


Рис. 7. Интерфейс режимов шифрования

С помощью управляющих клавиш данного интерфейса обеспечивается размещение в соответствующих окнах адресов входного и выходного файлов и обращение к гистограммам этих файлов, что более подробно поясняется в разделе IV. Нажатием на клавиши, идентифицирующие примитивы, предусмотрена возможность включения (ON), или исключения (OFF) примитивов из процесса шифрования. По окончании работы программы на тело интерфейса выводится значение машинного времени, затрачиваемого на ту или иную операцию (зашифрования или расшифрования), и указывается энтропия и размер входного и выходного текстов.

IV. Анализ эффективности шифра. Важнейшим показателем качества поточных шифров является их способность генерировать псевдослучайную последовательность двоичных чисел, максимально приближенную по своим статистическим характеристикам к характеристикам *белого шума*. Двоичная дискретная ПСП обладает свойствами белого шума при выполнении, по крайней мере, следующих условий. Во-первых, последовательность должна быть *сбалансированной*, т.е. число нулей и единиц в ней является одинаковым. И, во-вторых, автокорреляционная функция потока, состоящего из нулей и единиц, описывается дельта-функцией Дирака. Таким образом, двоичный дискретный белый шум – это просто сбалансированная последовательность статистически независимых бинарных чисел.

Существуют различные критерии и подходы к оценке степени приближения ПСП, генерируемой поточным шифром, к белому шуму. Простейший из них предполагает построение гистограммы элементов ПСП, состоящих из фиксированного числа бит последовательности, и расчете на их основе энтропии генератора. Выберем в качестве элементов ПСП восьмибитные векторы (байты). Байты последовательности, формируемые генератором, могут находиться в одном и 256

состояний S, начиная с $S_0 = 00000000$ до $S_{255} = 11111111$. Нижний индекс i в обозначении S_i совпадает с десятичным значением состояния байта. Пусть n_i – частота S_i – байтов и $L = \sum_{i=0}^{255} S_i$ – общее число байтов ПСП. Энтропия H генератора ПСП определяется формулой Шеннона [13]

$$H = -\sum_{i=0}^{255} p_i \cdot \log_2 p_i, \qquad (6)$$

где $p_i = n_i / L$ – частость (статистическая вероятность) S_i – байтов.

Для того чтобы перевести SCSPS шифр в режим генератора ПСП, достаточно указать базовый ключ шифрования Key, а на вход шифра подать *пустой файл* некоторой фиксированной, но достаточно большой длины. Пустым будем называть файл данных, каждый бит которого равен 0. На рис. 8 показан пример гистограммы ПСП, образованной шифром SCSPS для таких параметров генератора: длина входного пустого файла составляет 100 Мбит (файл содержит 12.5 миллионов байтов, являющихся NUL символами кодировочной таблицы ASCII), а размер ключа шифрования Key равен 128 бит.

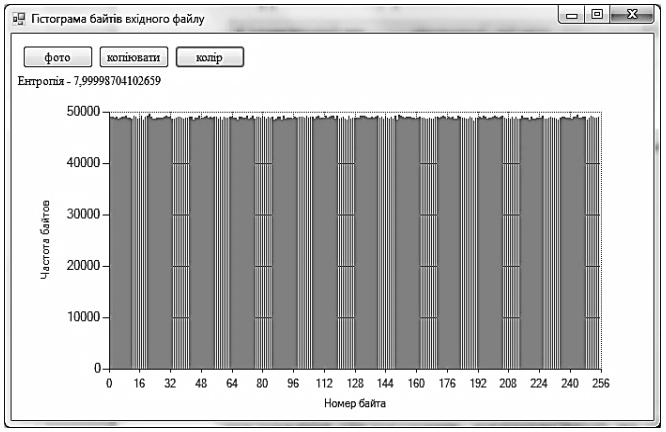


Рис. 8. Гистограмма ПСП объемом 100 Мбит

Частоты байтов, рассчитанные программой SCSPS-Universal (данная функция инициируется нажатием на клавишу «Гистограмма») для отображенных на рис. 5-7 параметров генератора ПСП, представлены на рис. 9. Номер i байта определяется суммой цифр, вписанных в ячейки строк (слева) и столбцов (сверху) указателей номеров байтов (обозначенных dec).

На основании приведенных данных по формуле (6) определена энтропия ПСП, которая составляет $H = 7.999987$ бит. Такое значение энтропии можно считать вполне удовлетворительным, поскольку ее максимальное значение, достигаемое при равномерном распределении статистических вероятностей p_i (когда $p_i = 1/256$), равно 8 бит. Таким образом, приходим к заключению о том, что по критерию максимума энтропии генерируемая SCSPS шифром псевдослучайная последовательность бинарных чисел достаточно близка к белому шуму.

Статистика байтів вхідного файлу

Ентропія - 7,99998704102659

dec	0	1	2	3	4	5	6	7	8	9
0	48691	48955	49002	48689	48985	48601	48793	48867	48936	49218
10	48689	48681	48592	49236	49051	48522	48853	49190	48390	48914
20	49214	49456	48917	48534	48606	48781	48787	48748	48841	48869
30	49083	48919	48927	48567	48563	48740	48901	48912	48844	48603
40	48727	48770	48954	48873	48370	48730	48784	49086	48524	48809
50	48945	49061	48723	48997	48739	48899	49042	48501	48882	48406
60	48934	48804	48745	49023	49041	48845	48693	48339	49010	48900
70	48832	48777	49147	48623	48732	49134	48614	48996	48944	48851
80	48890	48982	48536	48896	48733	48909	48386	48626	48959	48914
90	48403	49075	48625	48800	48720	48848	48530	48875	48829	49030
100	49047	48900	48818	49064	48806	48987	48936	48651	48996	49192
110	48757	48681	48708	49233	48842	49014	49105	49087	48652	49129
120	48542	48828	48950	48642	48382	49101	48613	48762	48863	48682
130	48700	49073	49079	49118	48899	48864	48728	48948	48813	48984
140	49134	48792	49035	48482	49036	48780	48664	49024	48653	49069
150	48469	49271	49161	48953	48802	48882	48995	49000	48701	48800
160	48644	48770	48933	48829	48794	48635	48532	48734	48516	48589
170	49034	49090	49026	49037	49001	49003	49010	49019	49777	49006
180	48567	48508	49216	48975	48786	48792	48667	48543	48941	48740
190	48272	48819	48752	49019	48721	49184	48888	48614	48789	48791
200	49019	49091	48888	48741	48992	49117	48709	48488	48850	48627
210	48881	48495	48901	48620	48655	49066	48840	48831	48741	48332
220	49004	48547	48610	48831	48813	48751	49248	48530	48551	48799
230	48900	48782	48720	48516	48474	48802	48946	48999	48821	48762
240	48854	48599	49052	48878	49268	48861	48830	48951	48937	48477
250	48748	49069	49005	48812	48842	48980	-	-	-	-

Рис. 9. Статистика байтов, сформированных шифром SCSPS в режиме генератора ПСП

Второй способ оценки качества ПСП основан на специальных системах статистического тестирования, в частности тестах Д. Кнута [14], DIEHART [15], CRYPT-SX [16], FIPS [17] и др. Однако самым распространенным среди них является набор статистический тестов NIST STS [18]. При тестировании генератора ПСП пакетом NIST вычисляются 188 (в отдельных версиях пакета – 189) статистических признаков, объединенных в 15 статистических групп. По результатам работы пакета определяется вероятностная мера P каждого признака, а их совокупность представляет собой *статистический портрет генератора.*

Пример статистического портрета псевдослучайной последовательности объемом 100 Мбит, образованной генератором на основе поточного SCSPS шифра (с длиной ключа *Key*, равным 128 бит), показан на рис. 10. Вероятности P для каждого статистического теста должны быть не менее 0,96015. Как следует из портрета, значение P только лишь одного теста близко к критическому уровню. А это означает, что полученные результаты тестирования можно считать вполне удовлетворительными, а генерируемую последовательность двоичных чисел – достаточно хорошо согласующуюся с белым шумом.

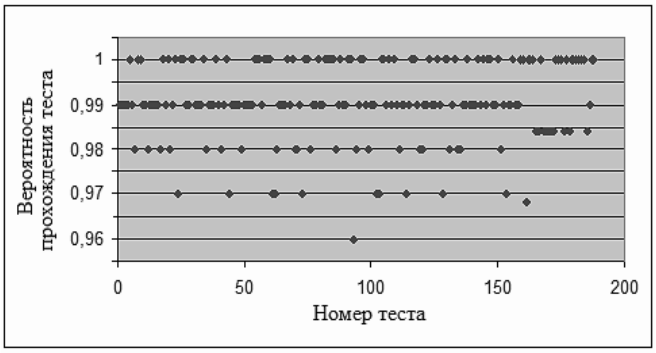


Рис. 10. Статистический портрет генератора ПСП на основе поточного SCSPS шифра

Как показали результаты машинного эксперимента переход к режиму SC2, также как и к SB2, не приводит к какому-либо значимому возрастанию энтропии шифротекста и на этом основании их нецелесообразно применять в SCSPS генераторах ПСП.

В табл. 1 приведены результаты оценок энтропии (H бит) ПСП длины 100 Мбит и затрат машинного времени (T сек) на формирование потока бинарных чисел SCSPS шифром в различных режимах генерации.

Таблица 1

Статистика файлов бинарных ПСП, сформированных поточным SCSPS шифром

Примитивы			Размер таблицы перестановок			
			8x8		16x16	
SC1	Perm	Shift	H	T	H	T
1	2	3	4	5	6	7
+	+	+	7.999749	0.72	7.999777	0.72
–	+	+	7.999985	0.56	7.999982	0.58
+	–	+	7.999777	0.58	7.999777	0.58
+	+	–	7.984262	0.49	7.993375	0.48
+	–	–	7.927370	0.35	7.927370	0.36
–	+	–	7.917181	0.32	7.917181	0.35
–	–	+	7.999986	0.44	7.999986	0.46

Во всех вариантах, представленных в табл. 1, генератор ПСП включает примитив Substitution в режиме SB1. Параметры моделирования выбраны такими: базовый 128 битный ключ *Key* равен 5B44B72AFF20D620971 A0F2442DF9E25; для примитива Substitution $\alpha = 00011011$, $\beta = 11100110$, $f = 100111001$, $\varphi = 101011111$ и $\omega = 01111011$.

Выводы. На основании проведенных исследований приходим к следующему заключению. Во-первых, рассеивающие свойства SCSPS генераторов ПСП, оцениваемые энтропией формируемых ими потоков бинарных чисел, оказываются практически инвариантными к порядкам перестановочных таблиц. На этом основании, а также с целью повышения скорости генерирования ПСП, рекомендуемый порядок перестановочных таблиц целесообразно выбрать равным 8x8. И, во-вторых, (это может показаться несколько неожиданным) генератор ПСП, построенный всего лишь на двух примитивах: Substitution (вариант SB1) и Shift, оказался (по критерию максимума энтропии H) более эффективным не только по сравнению с генератором, основанном на классической SP-сети Шеннона, но и с другими вариантами генераторов, представленных в табл. 1.

ЛИТЕРАТУРА

[1]. Асосков А.В. Поточные шифры / А.В. Асосков, М.А. Иванов, А.А. Мирский, А.А. Рузин и др. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.

[2]. Поточные шифры. Результаты зарубежной открытой криптологии. [Электронный ресурс] – Режим доступа: http://www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm

[3]. Поточный шифр A5. [Электронный ресурс] – Режим доступа: http://ru.wikipedia.org/wiki/A5

[4]. Поточный шифр RC4. [Электронный ресурс] – Режим доступа: http://ru.wikipedia. org/wiki/RC4

[5]. Описание протоколов SSL/TLS. Информационный документ. / Изд-во ООО "Крипто-Про", 2002. – С. 49. [Электронный ресурс] – Режим доступа: http://www.kryptopro.ru/sites/default/files/docs/TLS

[6]. WEP шифрование в WI-FI сетях. [Электронный ресурс] – Режим доступа: http://kavayii.blogspot.com/2010/01/wep-wi-fi.html

[7]. Поточный шифр Rabbit. [Электронный ресурс] – Режим доступа: http://ru. wikipedia.org/viki/Rabbit

[8]. Advanced Encryption Standard (AES) – FIPS 197 [Электронный ресурс] – Режим доступа: http://csrc. nist.gov/publications/fips/fips197/fips-197.pdf

[9]. Grey F. Pulse code communication / F. Grey. – Pat. USA, № 2632058, 1953.

[10]. Белецкий А.Я. Преобразования Грея. Монография в 2-х томах. /А.Я. Белецкий, А.А. Белецкий,

Е.А. Белецкий. Т.1. Основы теории. – К.: Кн. Изд-во НАУ, 2007. – 412 с.
[11]. Белецкий А.А. Программно-моделирующий комплекс криптографических AES-подобных примитивов нелинейной подстановки / А.А. Белецкий, А.Я. Белецкий, Д.А. Навроцкий, А.И. Семенюк // Захист інформації, № 1, 2014. – С 12-22.
[12]. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. / М.А. Иванов, И.В. Чугунков. – М: Изд-во КУДИЦ-ОБРАЗ, 2003. – 240 с.
[13]. Шеннон К. Работы по теории информации и кибернетики. – М.: ИЛ, 1963. – 829 с.
[14]. Кнут Д. Искусство программирования для ЭВМ. Получисленные алгоритмы. Т. 2. – М.: Мир, 1977. – 700 с.
[15]. Marsaglia G. DIEHART Statistical Test. [Электронный ресурс] – Режим доступа: http://stat. fsu.edu/ geo /diehart/html
[16]. Gustafson. H. Statistical Test Suit CRYPT-SX. [Электронный ресурс] – Режим доступа: http://www.istc.qut.edu.au/crypt
[17]. Federal Information Processing Standards Publication FIPS PUB 140-1. [Электронный ресурс] – Режим доступа: http://csrc.nist.gov/publications/ fips/fips1401.htm
[18]. Кравцов Г.О. NIST 800-22. Набор статистических тестов для генераторов случайных и псевдослучайных чисел для криптографических приложений. [Электронный ресурс] – Режим доступа: www.itsway.kiev.ua/pdf/Articles180106.pdf

REFERENCES

[1]. Asoskov A., Ivanov M., Mirskiy A., Ruzyne A. etc. (2003) "Stream ciphers" M.: KUDITS-OBRAZ, 336 p.
[2]. Stream ciphers. The results of foreign-covered cryptology. http://www.ssl.stu.neva.ru/psw/crypto/ potok/str_ciph.htm
[3]. Stream ciphers A5. http:// ru.wikipedia.org/wiki /A5
[4]. Stream ciphers RC4. http:// ru.wikipedia.org/wiki /RC4
[5]. Description of the protocols SSL / TLS. Informational onny document. / Acad LLC "Crypto-Pro" 2002, P. 49. http://www.kryptopro.ru/sites/default /files/docs/TLS
[6]. WEP encryption in WI-FI networks. http:// kavayii.blogspot.com/2010/01/wep-wi-fi.html
[7]. Stream ciphers Rabbit. http:// ru.wikipedia.org/ wiki/Rabbit
[8]. Advanced Encryption Standard (AES) – FIPS 197 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[9]. Grey F. (1953) Pulse code communication, Pat. USA, № 2632058.
[10]. Beletsky A.Y., Beletsky A.A., Beletsky E.A. (2007) "Gray conversion. Monograph in 2 vols. V.1. Fundamentals of the theory." K.: Book House NAU, 412 p.
[11]. Beletsky A.A., Beletsky A.J., Navrotskyi D.A., Semeniuk A.I. (2014) "Software-modeling complex cryptographic primitives like AES-nonlinear substitution" Ukrainian Information Security Research Journal, V.16, №1, P. 12-22.
[12]. Ivanov M.A., Chugunkov I.V. (2003) "Theory, application and evaluation of the quality of pseudorandom sequences" M: KUDITS-OBRAZ, 240 p.
[13]. Shannon K. (1963) "Works on information theory and cybernetics" Moscow: IL, 829 p.
[14]. Knuth D. (1977) "The Art of Computer Programming. Seminumerical algorithms. T. 2." New York: Wiley, 700 p.
[15]. Marsaglia G. DIEHART Statistical Test. http://stat. fsu.edu/~geo/diehart/html
[16]. Gustafson. H. Statistical Test Suit CRYPT-SX. http://www.istc.qut.edu.au/crypt
[17]. Federal Information Processing Standards Publication FIPS PUB 140-1. http://csrc.nist.gov/ publications/fips/fips1401.htm
[18]. Kravtsov G.O. NIST 800-22. A set of statistical tests of random and pseudo random numbers for cryptographic applications. www.itsway.kiev.ua/ pdf/ Articles180106.pdf

ПРОГРАМНО-МОДЕЛЮЮЧИЙ КОМПЛЕКС SCSPS АЛГОРИТМУ ПОТОЧНОГО ШИФРУВАННЯ

Основу SCSPS алгоритму поточного шифрування утворюють шенноновські примітиви нелінійної підстановки (Substitution) і перестановки (Permutation), або так звані SP-мережі, які доповнюються примітивами «ковзного кодування» (SlideCode) та стохастичного циклічного зсуву (Shift). Поточне шифрування здійснюється порозрядним додаванням за модулем 2 блоків тексту, що шифруються, розмір яких складає 128, 192 або 256 біт, з рівними по довжині блоками двійкових псевдовипадкових чисел (ключами, або гаммами). Потік гамм виробляється сукупністю криптографічних перетворень секретного базового ключа шифрування. Моделюючий комплекс допускає можливість виключення одного або декількох примітивів з алгоритму шифрування. Проведено аналіз ефективності SCSPS алгоритму.

Ключові слова: криптографічні примітиви, поточні шифри, програмно-моделюючий комплекс.

SOFTWARE-MODELING COMPLEX SCSPS STREAM ENCRYPTION ALGORITHM

Basis stream encryption algorithm SCSPS form Shannon primitives nonlinear Substitution and Permutations primitives, as well as SP-networks, supplemented by primitives of “moving coding” and stochastic cyclic Shift. Stream encryption is performed bitwise addition modulo 2 blocks ciphered text size is 128, 192 or 256 bits, with equal length blocks of binary pseudorandom numbers (keys or gammas). Flow gammas produced a set of cryptographic transformations underlying secret encryption key. Modeling complex is subject to exclusion of one or more entities from the encryption algorithm. The analysis of efficiency SCSPS algorithm.

Keywords: cryptographic primitives, stream ciphers, software-modeling complex.

Белецкий Анатолий Яковлевич, доктор технических наук, профессор кафедры электроники Национального авиационного университета.
E-mail: abelnau@ukr.net
Білецький Анатолій Якович, доктор технічних наук, професор кафедри електроніки Національного авіаційного університету.
Beletsky Anatoly, Doctor of Science, Professor of Department Electronics of National Aviation University.

Навроцький Денис Олександрович, аспірант кафедри електроніки Національного авіаційного університету.
E-mail: sg6336@yandex.ua
Навроцкий Денис Александрович, аспирант кафедры электроники Национального авиационного университета.
Navrotskyi Denys, Postgraduate student of Department Electronics of National Aviation University.

Семенюк Олександр Іванович, студент кафедри електроніки Національного авіаційного університету.
E-mail: sovist9@mail.ru
Семенюк Александр Иванович, студент кафедры электроники Национального авиационного университета.
Semenjuk Alexander, Student of Department Electronics of National Aviation University.

УДК 004.056.5

ЗАГРОЗИ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ: ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Олександр Юдін, Сергій Бучик

Проведено аналіз існуючого нормативно-правового та законодавчого забезпечення, вітчизняних і міжнародних стандартів галузі «Інформаційна безпека». Детально розглянуто напрями, що регламентують питання поняття загрози, загрози інформаційній безпеці, загрози інформації. Проведено нормативно-правовий аналіз, на основі якого приведено найповніше поняття загроз державним інформаційним ресурсам та атаки на державні інформаційні ресурси. Визначено недоліки та встановлено відсутність загального системного підходу (методології побудови) до формування моделі порушника і моделі загроз державним інформаційним ресурсам на базі вітчизняних і міжнародних вимог і стандартів.

Ключові слова: *державні інформаційні ресурси, загроза, загроза інформації, загроза державним інформаційним ресурсам, атака на державні інформаційні ресурси.*

Вступ. Стрімке зростання новітніх технологій, а також розвиток інфраструктури інформаційно-комунікаційних мереж державного та загального призначення, призвело до створення інтегрованого інформаційного простору держави та всього суспільства. Інформаційні технології знаходять ширше застосування у таких сферах, як: державні системи управління, фінансовий обіг і ринок цінних паперів, розвинута система електронних платежів, система послуг зв'язку та телебачення, системи управління транспортом, високотехнологічні виробництва (особливо атомних, хімічних тощо) та ін. Будь-яке несанкціоноване та противоправне втручання у інформаційний простір наведених сфер життєдіяльності держави й суспільства може призвести до тяжких та не передбачуваних наслідків.

Особливого значення вирішення проблеми інформаційної безпеки державних інформаційних ресурсів (ДІР) набуває у сучасних умовах глобалізації інформаційних процесів, а також в умовах цілеспрямованих дій ряду розвинених держав та ІТ- корпорацій досягти домінування у світовому інформаційному просторі й на ринку ІТ- послуг.

Міжнародний та вітчизняний досвід демонструє, що забезпечення безпеки інформаційних ресурсів повинно носити комплексний характер. Однак, організація процесів безпеки має бути не просто комплексною складовою, але ще й засновуватися враховуючи всебічний аналіз можливих негативних загроз ДІР та їх можливих наслідків.

Здійснюючи аналіз напрямків забезпечення інформаційної безпеки держави, які являють нормативно-правові, організаційні, інженерно-технічні категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, особисте значення набуває такий напрямок, як *правовий. Правовий захист ДІР* повинен формуватися на тлі загальної та спеціальної законодавчої бази держа-