ШИФРОВАНИЕ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА С ИСПОЛЬЗОВАНИЕМ СИНГУЛЯРНОГО СПЕКТРАЛЬНОГО АНАЛИЗА

А. В. Сидоренко, И. В. Шакинко

ВВЕДЕНИЕ

Современные информационные технологии находят все более широкое применение в телекоммуникационных системах. При этом существенную роль начинают играть вопросы защиты информации. Весьма актуальной становится задача разработки и внедрения надежных методов и средств в области защиты информации для обеспечения ее целостности и конфиденциальности. Использование динамического хаоса при шифровании данных предъявляет новые требования к обеспечению надёжности, качественности шифра.

Динамический хаос – нерегулярные колебания, рождаемые нелинейными процессами, для которых динамические законы однозначно определяют эволюцию состояния системы во времени по известной предыстории.

Целью работы является использование метода сингулярного спектрального анализа для получения количественных и качественных параметров выходных последовательностей зашифрованных сообщений с использованием динамического хаоса.

МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЙ

В качестве схемы алгоритма шифрования используется сеть Фейстеля, которая представляет собой определённую многократно повторяющуюся структуру, называемую ячейкой Фейстеля. При переходе от одной ячейки к другой меняется секретный ключ. В нашей работе число итераций z изменялось от одной до 1024. Для формирования нового итерационного ключа использовалось хаотическое отображение «пилообразное» ($F(x) = (Ax)\mathrm{mod}(M\text{-}1)$, где A – параметр отображения, M – мощность). Для проведения исследований в нашей работе выбраны 2 режима шифрования: обратная связь по выходу OFB (Output Feed Back) и сцепление блоков шифра CBC (Cipher Block Chaining) [2, с. 223]. Для анализа зашифрованных сообщений использовался метод «сингулярный спектральный анализ», базовый алгоритм которого включает в себя следующие этапы [1]:

1. Пусть задан временной ряд $\{x_i\}^N{}_{i=1}$, образованный последовательностью N равноотстоящих значений некоторой функции $f(t)$. Производится развертка одномерного ряда в многомерный.

$$X = (x)_{i,j=1}^{k,M} = \begin{pmatrix} x_1 & x_2 & x_3 & & x_M \\ x_2 & x_3 & x_4 & \cdots & x_{M+1} \\ x_3 & x_4 & x_5 & & x_{M+2} \\ & \vdots & & \ddots & \vdots \\ x_k & x_{k+1} & x_{k+2} & \cdots & x_N \end{pmatrix}, \quad (1)$$

2. Сингулярное разложение выборочной ковариационной матрицы. Вычисляется матрица $V = \frac{1}{k} X^T X$. Определяются собственные числа и собственные вектора матрицы V, т. е. ее разложение $V = P\Lambda P^T$, где Λ – диагональная матрица, собственных чисел, а P – ортогональная матрица собственных векторов матрицы V.

3. Отбор главных компонент**.** С учетом свойств матрицы P матрицу ряда можно представить в виде $X = YP^T$.

4. Восстановление одномерного ряда. Восстановление проводится по главным компонентам, если при применении формулы $X = Y * P$ матрица получена из матрицы $Y*$ обнулением всех не входящих в набор компонент.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Анализу подвергались реализации текстовых сообщений длиной N=10 000, длина гусеницы M=1000. Уровень главных компонент I определялся собственными значениями матрицы, нормированными на сумму всех значений. Результаты, полученные при использовании для анализа открытого текста и зашифрованных сообщений метода сингулярного спектрального анализа, приведены в таблице. Как видно из таблицы, уровень главных компонент для алгоритма шифрования по структуре CBC примерно совпадает с соответствующим показателем для открытого текста. Для алгоритма шифрования по структуре OFB уровень главных компонент превосходит данный показатель примерно в 10 раз. График зависимости уровня главных компонент I от числа итераций z, приведенный на рис.1, показывает, что данные соотношения сохраняются при различном числе итераций.

Таблица

Уровень главных компонент I (в процентах) открытого и зашифрованных текстов для различного числа итераций

число итераций	режим шифрования		открытый текст
	CBC	OFB	
1	0,3628	2,2948	0,353
4	0,2535	3,6462	
16	0,2416	3,9938	
128	0,2216	3,6462	
1024	0,2353	3,5264	

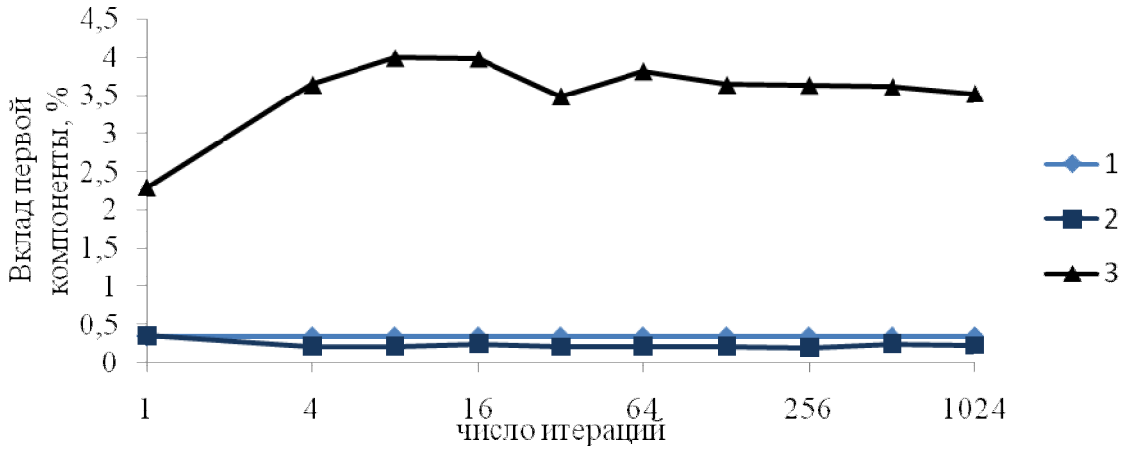

Рис.1. График зависимости уровня первых главных компонент *I* от числа итераций *z*: 1 – для открытого текста; 2 – при режиме шифрования CBC; 3 – при режиме шифрования OFB

Визуально для определения наличия детерминизма в исследуемых реализациях используется построение фазовых диаграмм, представляющие собой отложенные по осям x и y значения собственных векторов. Для фазовых диаграмм, полученных для зашифрованных сообщений при использовании алгоритма шифрования по структуре CBC, наблюдается «зашумлённость». В фазовых диаграммах при использовании алгоритма шифрования по структуре OFB отмечается наличие структурированности, что свидетельствует о наличии детерминизма в исследуемых реализациях.

ЗАКЛЮЧЕНИЕ

В результате проведенной работы установлено, что метод сингулярного спектрального анализа позволяет проанализировать количественно (по уровню главных компонент) и качественно (в виде фазовых диаграмм) выходные последовательности алгоритма шифрования на основе динамического хаоса. Значения параметров, определённые методом сингулярного спектрального анализа, включая уровень главных компонент,

отличаются численно и качественно для открытого текста и зашифрованных сообщений при режимах шифрования OFB и CBC.

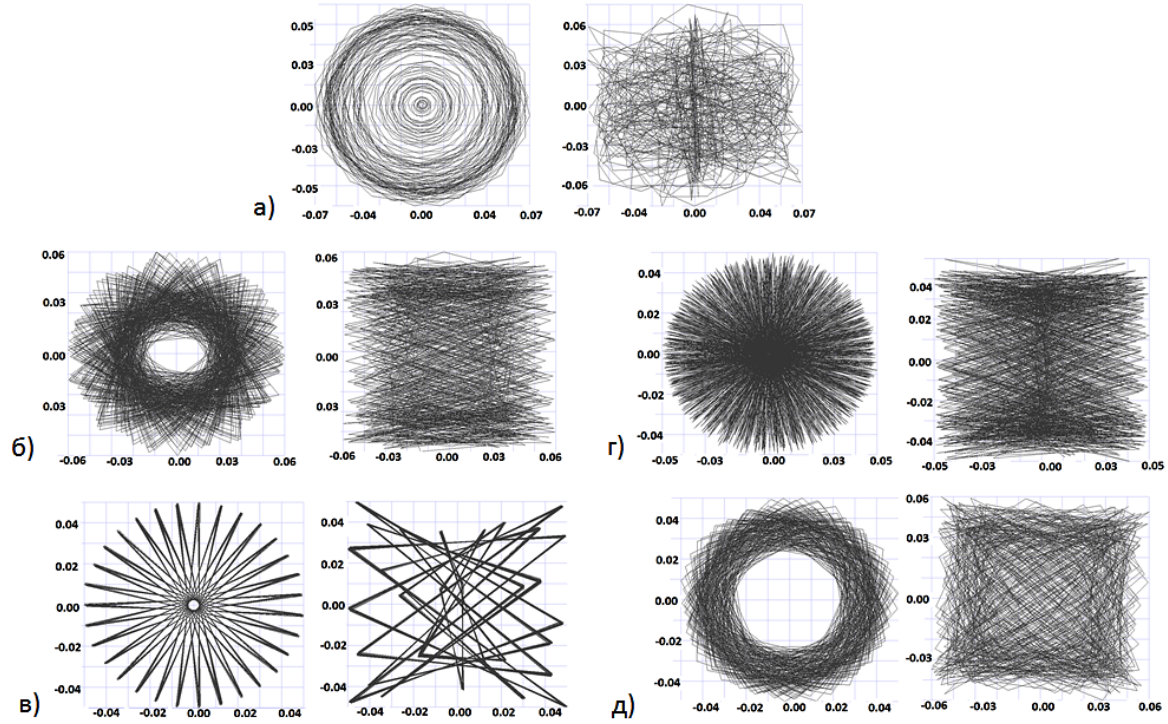

Рис. 2. Фазовые диаграммы пар собственных векторов с номерами 1000 и 999, 1000 и 998: а) – для открытого текста; б) – для алгоритма шифрования на основе динамического хаоса при режиме шифрования CBC; в) – для алгоритма шифрования на основе динамического хаоса при режиме шифрования OFB; г) – для алгоритма шифрования desпри режиме шифрования CBC; д) – для алгоритма шифрования des при режиме шифрования OFB

Литература

1. Главные компоненты временных рядов: метод "Гусеница". Под ред. Д. Л. Данилова и А. А. Жиглявского. Спб.: Спб. университет, 1997
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2005.

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ БЕСПРОВОДНЫМИ ДАТЧИКАМИ

А. Л. Труханович, О. А. Одноклубов

С каждым годом в мире все большую важность приобретают разнообразные системы автоматического управления. Обеспечение в помещении определенной температуры и влажности, обработка датчиков при навигации для сельского хозяйства, оповещение владельца автотранспорта о местоположении транспортных средств – это сферы, в которых автоматизация является востребованной. И для ее реализации необходима система мониторинга, которая бы опрашивала датчики и от-