УДК 004.056:061.068

ЛАВИННЫЙ ЭФФЕКТ В АЛГОРИТМАХ ШИФРОВАНИЯ НА ОСНОВЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ

К.С. МУЛЯРЧИК

Белорусский государственный университет
Независимости, 4, Минск, 220030, Беларусь

Поступила в редакцию 28 июня 2013

Проведено исследование лавинного эффекта в разрабатываемом алгоритме шифрования на основе дискретных хаотических отображений. Лавинный эффект проанализирован в дискретном тент-отображении, а также в базовом преобразовании на основе сети Фейстеля, где нелинейной функцией явилось указанное отображение. В каждом случае выполнен анализ пары «входное значение – выходное значение» и пары «управляющий параметр – выходное значение». Установлено, что при определенных условиях алгоритм шифрования удовлетворяет требованиям лавинного критерия для обеспечения стойкости к дифференциальному криптоанализу.

Ключевые слова: алгоритмы шифрования, динамический хаос, криптостойкость, лавинный эффект.

Введение

Интенсивное развитие информационных технологий и их проникновение во все сферы человеческой деятельности поднимает на новый уровень вопросы защиты информации. Очевидной является потребность в разработке новых алгоритмов шифрования, совместимых с передовыми технологиями типа «облачных вычислений» и одновременно обеспечивающих высокую производительность и криптографическую стойкость. Актуальным на сегодняшний день направлением в современной криптографии является разработка алгоритмов шифрования на основе динамического хаоса. Принципиальная схожесть фундаментальных свойств динамического хаоса и криптографии, среди которых можно выделить чувствительность к начальным условиям и подобно случайному поведение траекторий в фазовом пространстве динамических систем, привлекает большое внимание исследователей к этому направлению [1, 2].

При разработке алгоритмов шифрования обязательным является проведение их анализа на стойкость к различным видам криптоатак. Так, анализ криптостойкости алгоритмов шифрования на основе динамического хаоса может проводиться с применением как стандартных, так и специализированных методов [1, 3]. Одними из наиболее распространенных в настоящее время стандартных методов являются атаки на основе линейного и дифференциального криптоанализа [4]. Суть последнего состоит в отслеживании изменения разности между значениями выходных бит (в зашифрованных данных) в зависимости от изменения входных бит (в исходных данных) на различных раундах базового преобразования. Необходимым условием обеспечения стойкости алгоритма шифрования к дифференциальному криптоанализу является наличие лавинного эффекта в базовом преобразовании.

Теоретический анализ

Лавинный эффект в преобразовании проявляется в значительном – «лавинном» – изменении бит в выходном значении преобразования при малом изменении бит во входном значении преобразования по сравнению с исходным значением. Хорошие диффузионные свойства алгоритма шифрования являются следствием, в том числе, лавинного эффекта.

Выделяют следующие критерии, основанные на лавинном эффекте [5]:

– лавинный критерий – требует изменения в среднем половины бит в выходном (зашифрованном) значении при изменении каждого отдельно взятого бита во входном (исходном) значении;

– строгий лавинный критерий – требует изменения с вероятностью 0,5 каждого отдельно взятого бита в выходном значении при изменении каждого отдельно взятого бита во входном значении.

Методика

Для характеристики степени лавинного эффекта в преобразовании определены и использованы лавинные параметры – численные значения отклонения вероятности изменения бит в выходном значении при изменении бит во входной последовательности от требуемого значения вероятности, равной 0,5 [5].

Для лавинного критерия значение лавинного параметра (ε_{A_i}) определяется выражением $\varepsilon_{A_i} = \left|2k_{AVAL}(i) - 1\right|$, где i – номер изменяемого бита во входном значении, $k_{AVAL}(i)$ – вероятность изменения половины бит в выходном значении при изменении i-го бита во входном значении по сравнению с выходным значением при исходном (неизмененном) входном значении.

Для строгого лавинного критерия значение лавинного параметра ($\varepsilon_{S_{i,j}}$) определяется выражением $\varepsilon_{S_{i,j}} = \left|2k_{SAC}(i,j) - 1\right|$, где i – номер изменяемого бита во входном значении, j – номер анализируемого бита в выходном значении, $k_{SAC}(i,j)$ – вероятность изменения j-го бита в выходном значении при изменении i-го бита во входном значении по сравнению с выходным значением при неизмененном входном значении.

Диапазон изменения указанных лавинных параметров лежит в промежутке от 0 до 1 включительно. При этом, чем меньше значение лавинного параметра, тем сильнее лавинный эффект в преобразовании.

В данной статье проанализирован лавинный эффект, наблюдающийся в дискретном тент-отображении и базовом преобразовании на основе сети Фейстеля, где в качестве нелинейной функции использовано указанное отображение.

Необходимо отметить, что результат работы (выходное значение) как дискретного хаотического отображения, так и базового преобразования зависит не только от входного значения, но и некоторого вспомогательного значения – управляющего параметра. В случае базового преобразования таким управляющим параметром является раундовый ключ, генерируемый из ключа шифрования. Следовательно, как для дискретного отображения, так и для базового преобразования, анализ лавинного эффекта выполнен:

– для пары «входное значение–выходное значение» (анализируется, как изменение входного значения влияет на изменение выходного значения преобразования при некотором фиксированном значении управляющего параметра);

– для пары «управляющий параметр–выходное значение» (анализируется, как изменение управляющего параметра влияет на изменение выходного значения преобразования при некотором фиксированном входном значении).

Экспериментальная часть

Схема основного шага разрабатываемого алгоритма шифрования представлена на рисунке 1. В качестве базового преобразования используется сеть Фейстеля, а в качестве нелинейной функции в сети Фейстеля используется дискретное хаотическое отображение.

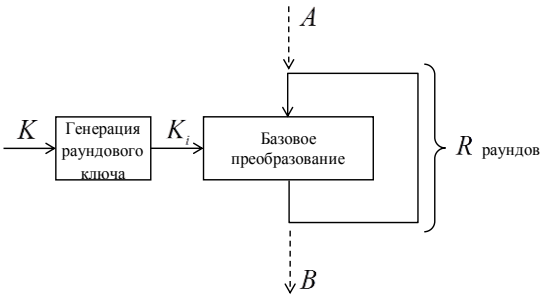


Рис. 1. Основной шаг алгоритма шифрования. На рисунке: A – значение открытого текста, B – значение шифртекста, K – ключ шифрования, K_i – раундовый ключ, R – количество раундов применения базового преобразования

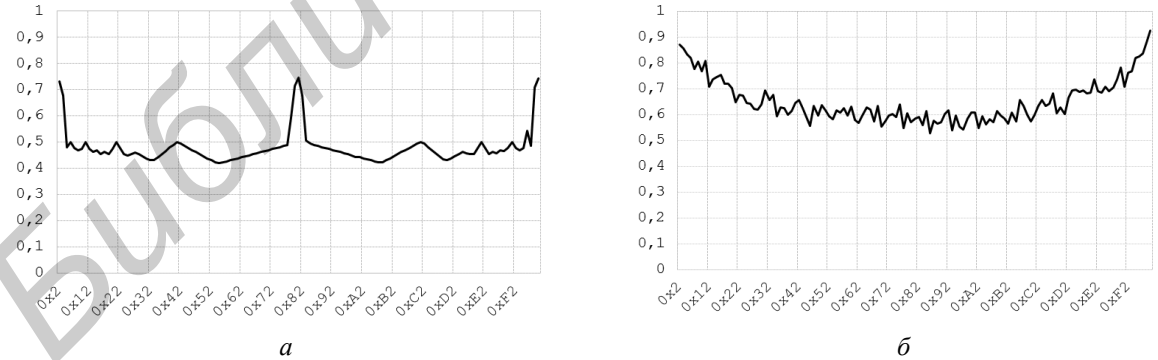
В данной статье рассматривается анализ лавинного эффекта при использовании дискретного тент-отображения. Данное отображение на целочисленном множестве $S = \{0, 1, ..., M-1\}$ мощности $M = 2^n$ (n – количество бит) задается выражением

$$F(X) = \begin{cases} \left\lceil \frac{M}{A} X \right\rceil, 0 \le X \le A, \\ \left\lfloor \frac{M}{M-A}(M-X) \right\rfloor + 1, A < X \le M-1 \end{cases},$$

где X – входное значение, A – управляющий параметр.

Результаты и их обсуждение

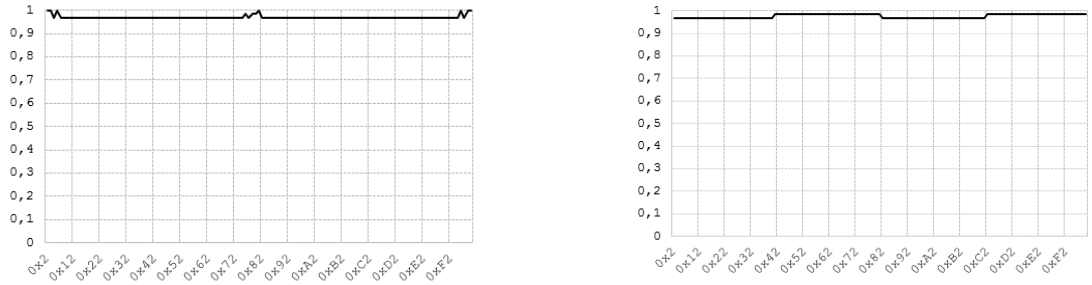
На рис. 2 представлены графики зависимости максимального значения лавинного параметра (ε_{A_i}) по всем входным битам в зависимости от значения управляющего параметра A (рис. 2, *а*) и входного значения X (рис. 2, *б*) дискретного тент-отображения. Здесь и далее мощность множества, на котором определено отображение, составляет 8 бит, если иное не указано явно.



а *б*

Рис. 2. Зависимость максимального значения лавинного параметра ε_{A_i} (ось *Y*) от управляющего параметра (ось *X*, рис. 2, *а*) и входного значения (ось *X*, рис. 2, *б*) для дискретного тент-отображения

На рис. 3 представлены графики зависимости максимального значения строгого лавинного параметра ($\varepsilon_{S_{i,j}}$) по всем номерам входных и выходных бит в зависимости от значения управляющего параметра A (рис. 3, *а*) и входного значения X (рис. 3, *б*) дискретного тент-отображения.

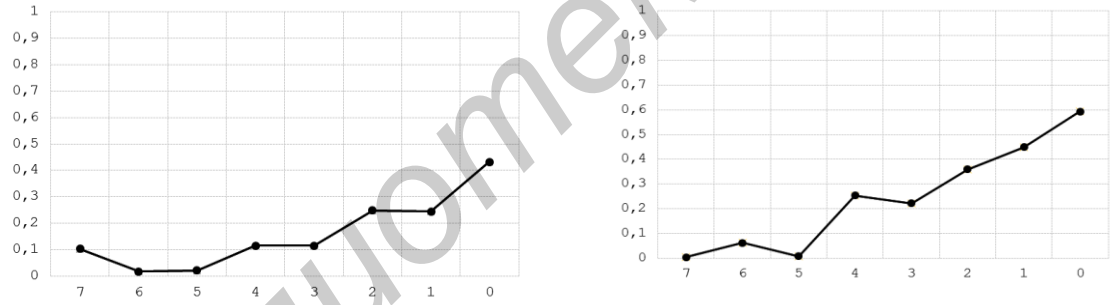


а *б*

Рис. 3. Зависимость максимального значения строгого лавинного параметра $\varepsilon_{S_{i,j}}$ (ось *Y*) от управляющего параметра (ось *X*, рис. 3, *а*) и входного значения (ось *X*, рис. 3, *б*) для дискретного тент-отображения

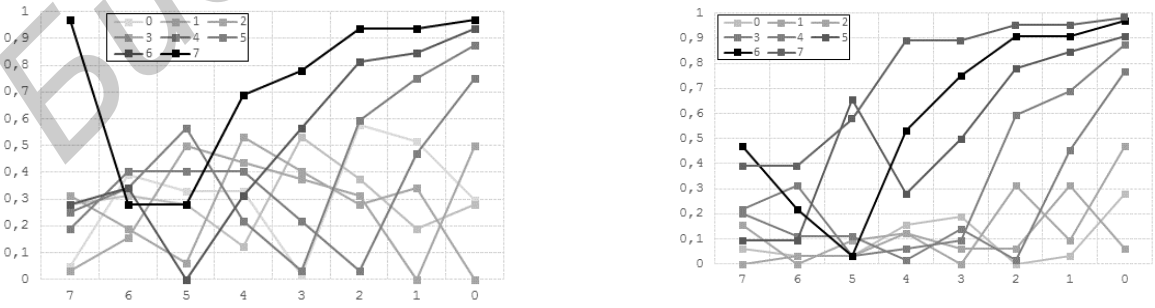
Проанализировав данные графики можно видеть, что минимальное значение лавинного параметра не опускается ниже значения 0,4, а минимальное значение строгого лавинного параметра не опускается ниже значения 0,9 для любых входных значений или управляющих параметров диапазона, соответствующего указанной мощности множества. На основании этого можно заключить, что дискретное тент-отображение в целом обладает слабыми лавинными свойствами.

На следующем этапе проведено более детальное исследование лавинного эффекта, поскольку функция выбора максимального значения «скрывает» все детали поведения тент-отображения. Так, на рис. 4 представлены зависимости значения лавинного параметра (ε_{A_i}) от номера входного бита при фиксированном значении управляющего параметра $A = 0{\times}52$ (рис. 4, *а*) и фиксированном входном значении $X = 0{\times}52$ (рис. 4, *б*). На рис. 5 представлены зависимости значений строгого лавинного параметра ($\varepsilon_{S_{i,j}}$) для разных номеров выходных бит от номера входного бита при указанных выше фиксированных значениях.



а *б*

Рис. 4. Зависимости значения лавинного параметра (ось *Y*) от номера входного бита (ось *X*) для управляющего параметра $A = 0{\times}52$ (рис.4, *а*) и входного значения $X = 0{\times}52$ (рис.4, *б*) дискретного тент-отображения



а *б*

Рис. 5. Зависимости значения строгого лавинного параметра (ось *Y*) от номера входного бита (ось *X*) для управляющего параметра $A = 0{\times}52$ (рис.5, *а*) и входного значения $X = 0{\times}52$ (рис.5, *б*) для разных номеров выходных бит дискретного тент-отображения

На представленных на графиках зависимостях заметно уменьшение значения лавинного параметра и строго лавинного параметра при увеличении номера изменяемого бита во входном значении. Таким образом, в тент-отображении более сильный лавинный эффект наблюдается при изменении старших входных бит (биты 5–8), чем при изменении младших бит (биты 1–4).

На основании анализа данного типа зависимостей обуславливается выбор в алгоритме шифрования при использовании в нем данного дискретного хаотического отображения вида базового преобразования и схемы генерации раундовых ключей, обеспечивающих наиболее сильный лавинный эффект. А именно, анализ характера лавинного эффекта в паре «входное значение – выходное значение» дискретного хаотического отображения определяет выбор вида базового преобразования, а в паре «управляющий параметр – выходное значение» – выбор схемы генерации раундовых ключей.

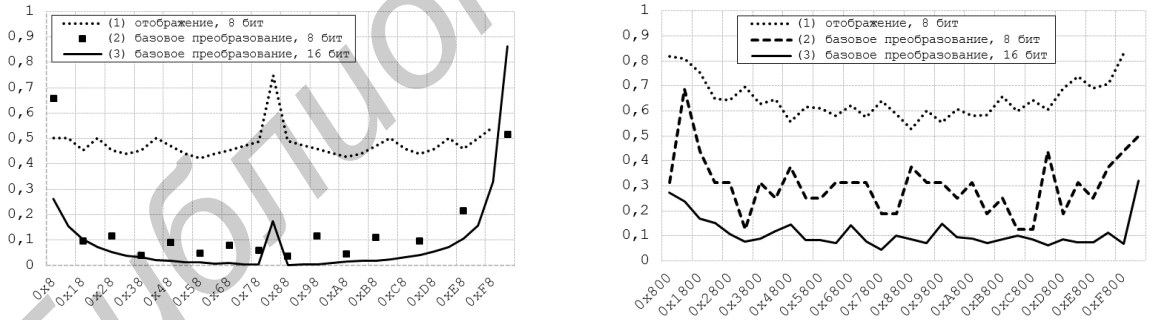
В случае с дискретным тент-отображением установлено, что подходящим видом базового преобразования является сеть Фейстеля. Далее приведен анализ лавинного эффекта в базовом преобразовании на основе сети Фейстеля, где в качестве нелинейной функции использовано дискретное тент-отображение.

В силу особенностей структуры сети Фейстеля можно выделить два варианта для сравнения лавинного эффекта в дискретном тент-отображении и при его использовании в качестве нелинейной функции в базовом преобразовании. Так, отображение на множестве мощности 8 бит можно сравнить с:

– базовым преобразованием на множестве мощности 8 бит, при этом само отображение определено на множестве 4 бит – в этом случае сохраняется множество на котором сравнивается два преобразования;

– базовым преобразованием на множестве мощности 16 бит, при этом само отображение определено на множестве 8 бит – в этом случае сохраняется множество, на котором определено исходное отображение и используемое в базовом преобразовании.

На рис. 6 представлены графики зависимости максимального значения лавинного параметра (ε_{A_i}) по всем входным битам в зависимости от значения управляющего параметра (рис. 6, *а*) и входного значения (рис. 6, *б*) базового преобразования и исходного тент-отображения. Процедура генерации раундового ключа в данном случае заключалась в применении исходного ключа шифрования на каждом раунде. Количество раундов базового преобразования равняется 10.



а *б*

Рис. 6. Зависимость максимального значения лавинного параметра (ось *Y*) от управляющего параметра (ось *X*, рис. 6, *а*) и входного значения (ось *X*, рис. 6, *б*) исходного тент-отображения на множестве мощности 8 бит (кривая 1, точки), базового преобразования на множестве мощности 8 бит (кривая 2, квадрат/пунктир), базового преобразования на множестве мощности 16 бит (кривая 3, сплошная)

Из данных графических зависимостей следует, что в базовом преобразовании на основе сети Фейстеля с дискретным тент-отображением в определенных диапазонах значений управляющего параметра и входного значения наблюдается более сильный лавинный эффект, чем в исходном отображении. Так, в диапазоне значений управляющего параметра 0×18 – 0×78 и 0×88 – 0×E8 соответствующие значения лавинного параметра (ε_{A_i}) для базового преобразования заключены в интервале 0–0,1, а для исходного отображения – в интервале 0,4–0,5. Меньшее значение лавинного параметра свидетельствует о более сильном лавинном

эффекте. В диапазоне входных значений 0×2800 – 0×F800 соответствующие значения лавинного параметра (ε_{A_i}) для базового преобразования заключены в интервале 0,05–0,15, а для исходного отображения – в интервале 0,5–0,75.

Таким образом, в указанных диапазонах входных значений и значений управляющего праметра можно говорить об удовлетворении базовым преобразованием на основе сети Фейстеля и дискретного тент-отображения требованиям лавинного критерия для обеспечения стойкости к дифференциальному криптоанализу.

Заключение

Проведен анализ лавинного эффекта в дискретном тент-отображении и базовом преобразовании на основе сети Фейстеля, где нелинейной функцией является указанное отображение. Выбор сети Фейстеля в качестве вида базового преобразования при использовании в нем дискретного тент-отображения обоснован неравномерной зависимостью лавинного параметра от номера бита во входном значении отображения. В определенных диапазонах входных значений и значений управляющего параметра базовое преобразование на основе сети Фейстеля и дискретного тент-отображения удовлетворяет требованиям лавинного критерия для обеспечения стойкости к дифференциальному криптоанализу.

THE AVALANCHE EFFECT IN ENCRYPTION ALGORITHMS BASED ON THE DISCRETE CHAOTIC MAPS

K.S. MULYARCHIK

Abstract

The avalance effect has been investigated in an encryption algorithm being developed on the basis of the discrete chaotic maps. The avalanche effect has been analyzed in a discrete tent map and in the basic transformation based on the Feistel network with the use of the indicated map as a nonlinear function. In both cases, the analysis has been conducted in pairs “input value – output value” and “control parameter – output value”. It has been stated that under certain conditions the developed encryption algorithm meets the requirements of the avalance

Список литературы

1. *Sidorenko A.V., Myulyarchik K.S.* // Nonlinear Phenomena in Complex Systems. 2012. Vol. 16, № 1. P. 33–41.
2. *Сидоренко А.В, Мулярчик К.С.* // Тез. докл. X Бел.-росс. НТК «Технические средства защиты информации». Минск, 29–30 мая 2012 г. С. 50.
3. *Heys H.M.* //Cryptologia. 2002. Т. 26, № 3. С. 189–221.
4. *Kocarev L.* // Circuits and Systems Magazine, IEEE. 2001. Т. 1, № 3. С. 6–21.
5. *Vergili I., Yücel M. D.* // Turk J Elec Engin. 2001. Т. 9, №. 2. С. 137–145.