УДК 681.3.06:519.248.681

П. Ю. Костенко, А. В. Антонов, С. И. Сиващенко
Харьковский университет Воздушных Сил им. Ивана Кожедуба
ул. Сумская, 77/79, 61023 Харьков, Украина

Решение обратной задачи хаотической динамики как наиболее эффективный метод анализа криптографической системы с открытым ключом

Рассмотрен подход к решению задачи защиты информации в компьютерных системах и сетях, использующий достижения хаотической динамики. Предложена криптографическая система с открытым ключом, функционирующая как хаотическая динамическая система. Показано, что наиболее эффективный метод криптоанализа предложенной системы основан на решении обратной задачи хаотической динамики и имеет экспоненциальную зависимость сложности от длины ключа.

Ключевые слова: *криптография с открытым ключом, хаотическая динамика, обратная задача хаотической динамики, сложность криптоанализа.*

Один из новых подходов к совершенствованию криптосистем основан на их рассмотрении с позиций хаотической динамики [1, 2]. При этом можно единообразно оценить как существующие криптосистемы, так и вновь разрабатываемые. Кроме того, есть основания утверждать, что решения задач защиты информации в компьютерных системах и сетях с использованием методов хаотической динамики могут оказаться достаточно эффективными с точки зрения их криптостойкости. Разработке криптосистем с позиций хаотической динамики посвящены работы зарубежных авторов, например [3–5].

Особенно актуальными для больших информационно-коммуникационных систем и сетей являются криптосистемы с открытым ключом [6]. В настоящее время схемой шифрования с открытым ключом, получившей наибольшее признание и распространение, является RSA [7]. Она используется для обмена ключами, создания цифровой подписи и шифрования данных. Применяются также стандарт цифровой подписи DSS [8], схемы Эль-Гамаля [9], Шнорра [10], криптопреобразования в группе точек эллиптических кривых [11] и др. Дискретные преобразования, применяемые в некоторых из них, можно встретить и в хаотической динамике. Их криптостойкость основана на «вычислительной сложности» криптоана-

лиза теоретико-числовых алгоритмов. Однако «вычислительная сложность» зависит от развития математических методов решения теоретико-числовых задач (например, разложения чисел на простые множители, дискретного логарифмирования), что делает эти системы потенциально уязвимыми [12–14]. Поэтому разработка потенциально стойкой криптосистемы с открытым ключом в современной криптографии (в том числе и методами нелинейной динамики) представляется актуальной задачей.

В работе предложена криптосистема с открытым ключом, функционирующая как хаотическая динамическая система, криптостойкость которой основана на неоднозначности обращения хаотического отображения (оценки его порядка) в случае незнания личного ключа.

Цель работы — показать, что решение обратной задачи хаотической динамики является наиболее эффективным методом криптоанализа предложенной системы.

Хаотическая динамическая система задается оператором эволюции системы (отображением). Отображение можно задать в форме рекуррентного уравнения — новое значение состояния динамической системы определяется по предыдущему. В режиме развитого хаоса состояние системы становится трудно прогнозируемо и может быть описано в текущий момент времени инвариантной плотностью вероятности.

Для некоторых систем хаотическое решение рекуррентного уравнения можно записать в явном виде с помощью формулы [15]:

$$X_n = Щ(иTk^n),$$

где $Ψ(t)$ — периодическая функция (тригонометрическая, эллиптическая и др.); k — параметр, определяющий порядок отображения; T — период функции $Щ(t)$; $x_0 = Щ(иT)$ — начальное значение хаотической системы (и — вещественное значение, удовлетворяющее данному условию). Конкретные формы записи для соответствующих отображений можно найти в [15]. Степень хаотичности системы характеризуется показателем Ляпунова: $\lambda = \ln(k)$ [16].

Важной особенностью некоторых отображений является так называемое полугрупповое свойство

$$\Psi_r(\Psi_s(t)) = \Psi_{r-s}(t), \qquad (1)$$

и его следствие — свойство коммутативности:

$$\Psi_r(\Psi_s(t)) = \Psi_s(\Psi_r(t)). \qquad (2)$$

Рекуррентное уравнение для двухэлементного кусочно-линейного отображения задается в виде:

$$x_{n+1} = \begin{cases} \dfrac{x_n}{a}, & 0 \le x_n < a, \\ \dfrac{1-x_n}{1-a}, & a \le x_n \le 1, \end{cases}$$

где n — натуральное число; x и a — вещественные числа, принимающие значения на интервале $(0,1)$. Параметр a определяет границы интервалов $(0,a]$ и $(a,1)$ задания элементов отображения, и часто называется управляющим.

Для предельного значения $a = 1/2$ решение рекуррентного уравнения записывается в явном виде с помощью формулы:

$$x_n = \frac{1}{\pi}\arccos(\cos(2^n \pi\, x_0)).$$

Здесь x_0 — начальное значение.

В общем случае отображение можно записать в виде:

$$T_k(x) = \frac{1}{\pi}\arccos\left(\cos\left(k\pi x\right)\right),$$

где k — порядок хаотического отображения, который определяет число его элементов.

Для кусочно-линейного отображения при целых значениях порядка справедливы свойства (1) и (2). Рассмотрим криптографическое приложение отображения $T_k(x)$.

Криптосистема с открытым ключом на основе кусочно-линейного отображения

Практически любая криптографическая система включает в себя три составляющих: формирование ключей, зашифрование и расшифрование сообщений.

Будем считать, что сообщение, подлежащее зашифрованию, представляется (кодируется) натуральным числом *M*. В двоичной системе счисления *M* записывается не более чем m битами. Тогда емкость множества возможных сообщений $V_M = M_{\max} = 2^m$.

Формирование ключей пользователем ***A*** включают в себя следующие основные этапы.

1. Генерирование простых чисел *P* и *Q*.

2. Нахождение неустойчивой неподвижной точки $X = T_N(X)$ отображения порядка $N = P \cdot Q$, которая должна находиться на интервале $\left(0,2^{-m}\right)$ определения первого элемента кусочно-линейного отображения порядка 2^m. Для этого параметры P и Q необходимо выбирать таким образом, чтобы выполнялось условие $N > 2^m$.

3. Вычисление и опубликование открытого ключа:

$$Y = T_P(X).$$

Значения X, P, Q, N являются секретными. Пара значений (X, Q) составляет личный ключ. Значения P и N в дальнейших вычислениях не используются.

Для зашифрования сообщения пользователь ***Б*** действует в следующем порядке.

1. Получает открытый ключ Y пользователя ***А***.
2. Вычисляет и отправляет пользователю ***А*** шифротекст:

$$C = T_M(Y).$$

Таким образом, порядок отображения принимает значение шифруемого сообщения M. Шифротекст C представляет собой вещественное число, принадлежащее интервалу $(0,1)$ определения отображения.

Процедура расшифрования сообщения пользователем ***А*** состоит в вычислении значения выражения:

$$\overset{C}{M} = \frac{\arccos\left(\cos\left(\pi T_Q(C)\right)\right)}{\pi X} = \frac{T_Q(C)}{X}, \qquad (3)$$

которое является оценкой сообщения M (порядка отображения).

Корректность работы криптосистемы основана на использовании полугрупповых (1) и коммутативных (2) свойств отображения

$$T_Q(C = T_M(Y = T_P(X))) = T_M(T_{N=P\cdot Q}(X)),$$

а также неустойчивых неподвижных точек $X = T_N(X)$, то есть:

$$T_Q(C) = T_M(X).$$

При выбранном интервале задания неустойчивых неподвижных точек X выполняется неравенство $MX \le 1$, с учетом которого

$$T_M(X) = \frac{1}{\pi}\arccos(\cos(\pi MX)) = MX.$$

Тогда для оценки $\overset{C}{M}$ справедливо выражение (3).

Информационная скрытность (стойкость) криптосистемы основана на неоднозначности определения открытого текста M непосредственным обращением

отображения $T_M(\ )$. По известным значениям открытого ключа Y и шифротекста C можно получить множество $\{\hat{M}\}$ оценок

$$\hat{M}_n = \frac{\pm \arccos(\cos(\pi C)) + 2\pi n}{\pi Y} = \pm \frac{\arccos(\cos(\pi C))}{\pi Y} + \frac{2}{Y} n = \\ = \pm \frac{C}{Y} + \frac{2}{Y} n,\ n = 0,1,..., \tag{4}$$

емкость $V_{\hat{M}} = 2 \cdot n_{\max} = \lfloor M_{\max} \cdot Y \rfloor$ которого зависит от значения открытого ключа Y и максимально возможного значения открытого текста $M_{\max} = 2^m$.

Множество $\{\hat{M}\}$ содержит одно натуральное значение $\hat{M} = M$ (остальные оценки — вещественные числа). Поэтому критерием выбора $\hat{M} = M$ из множества $\{\hat{M}\}$ является ее натуральное значение.

Покажем, что сложность *S* криптоанализа решением обратной задачи хаотической динамики (обращением хаотического отображения), определяемая числом итераций процедуры оценки искомого параметра, необходимых для успешного завершения криптоатаки, имеет экспоненциальную зависимость от длины ключа (блока открытого текста).

Сложность криптоанализа, а значит и стойкость криптосистемы, определяется емкостью $V_{\hat{M}}$ множества $\hat{M}$ и равна $S_M = V_{\hat{M}}/2$, где $V_{\hat{M}} = \lfloor 2^m \cdot Y \rfloor$.

Уменьшение сложности криптоанализа можно достичь учетом избыточности в сообщении M (эквивалентно уменьшению значения $M_{\max}$) и уменьшением значения Y. В предположении, что в M устранена возможная избыточность (все сообщения равновероятны), уменьшение сложности S_M достигается смещением значения открытого ключа Y к началу координат. Смещение достигается вычислением

$$\tilde{Y}_i = T_i(Y),\ i = 1, 2,...,$$

до тех пор, пока значение $\tilde{Y}_i$ не попадет в заданный интервал, принадлежащий окрестности начала координат. Для требуемой сложности S_M криптоанализа (см. (4)) верхняя граница области определения смещенного значения ключа $\tilde{Y}_i = T_i(Y)$ равна $y = 2 \cdot S_M / 2^m$. Сложность смещения открытого ключа Y в заданный интервал $(0, y]$ при условии, что емкость множества значений личного ключа $V_Q > V_M$, определяется статистическими свойствами хаотического отображения (вероятностью попадания $\tilde{Y}_i$ в интервал $(0, y]$) и равна значению $S_K = 1/y$.

Далее из выражения (4), пользуясь свойствами (1) и (2), получаем:

$$M^{C}_{Y} = \begin{cases} \dfrac{n + T_i(C)}{\widetilde{Y}_i}, & \text{если} \quad n - \text{четное}, \\ \dfrac{n - T_i(C) + 1}{\widetilde{Y}_i}, & \text{если} \quad n - \text{нечетное}. \end{cases} \tag{5}$$

Если границу y интервала выбрать из условия $y \le 2^{-m}$, то значение $\widetilde{Y}_i \in (0, y]$ и соответствующее ему значение i будут оценками личного ключа, которые позволяют определить порядок отображения M без разрешения неоднозначности, так как $n_{\max} = 0$. При этом для успешного криптоанализа не существенно соблюдение равенств $X = \widetilde{Y}_i$ и $Q = i$.

Суммарная сложность атаки равна:

$$S_{KM} = S_K + kS_M = 1/y + k\left[2^{m-1} y\right],$$

где k — число сообщений, криптоанализ которых необходимо выполнить. Вариациями y можно изменять значение сложности S_{KM}.

Представим сложность криптоанализа функцией $s(y,k,m) = 1/y + k \cdot 2^{m-1} y$, которая, как легко заметить, имеет один минимум при фиксированных значениях k и m. Оптимальное значение верхней границы интервала $(0, y]$, найденное из условия $\min\limits_{y} s(y,k,m)$, определяется выражением $y_{\text{opt}}(k,m) = \sqrt{2}\left(k \cdot 2^m\right)^{-1/2}$. Тогда соответствующее значение сложности равно:

$$s(k,m) = \frac{\left(k2^m\right)^{1/2}}{\sqrt{2}} + \sqrt{2}k2^{m-1}\left(k2^m\right)^{-1/2} = (2k)^{1/2} 2^{m/2} = \sqrt{2k} \cdot e^{(ln(2)/2)m} = O\left(\sqrt{k} \cdot e^{(ln(2)/2)m}\right). \tag{6}$$

Таким образом, зависимость $s(k,m)$ от длины m имеет экспоненциальный характер. Можно утверждать, что оценка сложности криптоанализа предложенной системы с использованием выражения (6) не меньше, а при росте k потенциально выше, сложности криптоанализа преобразований на эллиптических кривых. Значение $y_{\min}$ задается верхней границей интервала определения первого элемента отображения $T_M(Y)$. Максимальная сложность криптоанализа потока сообщений определяется сложностью атаки на ключ $S_{KM} = S_K = 2^{m-1}$ и достигается при условии $k \ge 2^{m-1}$, вытекающего из неравенства $y_{\text{opt}}(k,m) \le y_{\min} = 2^{-m}$.

Выражение (6) получено в предположении отсутствия более эффективного метода смещения открытого ключа Y в заданный интервал, чем последовательный перебор i в $\widetilde{Y}_i = T_i(Y)$. Однако можно предложить более эффективный метод решения этой задачи, в основе которого лежит пошаговое смещение открытого ключа.

Пошаговое смещение открытого ключа достигается вычислением значений

$$\widetilde{Y}_n = T_{\widetilde{Q}_n}\left(\widetilde{Y}_{n-1}\right),\ n = 1,2,\ldots,$$

где $\widetilde{Y}_0 = Y$, а $\widetilde{Q}_n = \left[2/\widetilde{Y}_{n-1}\right]$. Если полученное на шаге n значение $\widetilde{Y}_n > \widetilde{Y}_{n-1}/2$, то значение $\widetilde{Q}_n$ модифицируется как $\widetilde{Q}_n = \left[2/\widetilde{Y}_{n-1}\right]+1$, и вычисляется новое значение $\widetilde{Y}_n$ для шага n. Смещение проводится до тех пор, пока оценка $\widetilde{Y}_n$ не попадет в требуемый интервал. Далее значения $\widetilde{Y} = \widetilde{Y}_n$, $\widetilde{Q} = \prod_{i=1}^{n}\widetilde{Q}_i$ используются в выражении (5) для определения открытого текста. Оценим количество шагов $n_{\max}$, необходимых для успеха атаки и получаемое при этом значение $\widetilde{Q}$.

Очевидно, что за один шаг значение $\widetilde{Y}_n$ смещается в среднем в окрестность точки $\widetilde{Y}_{n-1}/4$, т.е. можно предположить, что:

$$\widetilde{Y}_n \approx \frac{1}{4}\widetilde{Y}_{n-1} = \left(\frac{1}{4}\right)^n \widetilde{Y}_0 = 2^{-2n}\widetilde{Y}_0.$$

Для полученной на шаге n оценки $\widetilde{Y}_n$ в среднем:

$$\widetilde{Q}_n = \left[\frac{2}{\widetilde{Y}_{n-1}}\right] = \left[\frac{2\cdot 2^{2(n-1)}}{\widetilde{Y}_0}\right] = \left[\frac{2^{2n-1}}{\widetilde{Y}_0}\right].$$

Соответственно на шаге n:

$$\widetilde{Q} = \prod_{i=1}^{n}\widetilde{Q}_i = \frac{2^n\left(2^{2(n-1)}\cdot 2^{2(n-2)}\cdot\ldots\cdot 2^2\right)}{\left(\widetilde{Y}_0\right)^n} = \frac{2^n\left(2^{2((n-1)+(n-2)+\ldots+1)}\right)}{\left(\widetilde{Y}_0\right)^n} = \frac{2^n\left(2^{n(n-1)}\right)}{\left(\widetilde{Y}_0\right)^n} = \left(\frac{2^n}{\widetilde{Y}_0}\right)^n.$$

Для эффективного противодействия криптоанализу решением обратной задачи хаотической динамики целесообразно выбирать значение открытого ключа Y в интервале $(2/3 - 0{,}25,\ 2/3 + 0{,}25)$. Соответственно для дальнейших рассуждений предположим, что $\widetilde{Y}_0 = Y = 1/2$. Тогда:

$$\widetilde{Q} = \left(\frac{2^n}{\widetilde{Y}_0}\right)^n \approx 2^{n(n+1)}.$$

Можно показать, что, если точность задания параметров криптосистемы выражать количеством бит, необходимым для их представления в формате двоичных чисел с фиксированной запятой, то для обеспечения однозначности криптопреобразований неустойчивые неподвижные точки X необходимо задавать с точ-

ностью не меньшей $4(m+1)$ бит. Такое значение получено в предположении, что параметры P и Q задаются $p = m+1$ и $q = m+1$ битами соответственно. Открытый ключ должен задаваться с точностью $3(m+1)$ бит, шифротекст — $2m+3$ битами.

Если полученная оценка $\widetilde{Q} > 2^{m+1}$, или $\widetilde{Q} \approx 2^{(m+1)+i}$, то ошибки округлений при вычислениях приведут к тому, что i последних бит оценки $\widetilde{M}$ будут неверными. В случае, если $\widetilde{Q} > 2^{2m}$, то в оценке $\widetilde{M}$ не содержится ни одного бита открытого текста.

Найдем n, для которого выполняется условие $\widetilde{Q} \le 2^{2m}$:

$$2^{n^2+n} \le 2^{2m},\ n^2+n \le 2m,\ n \le -\frac{1}{2}+\frac{1}{2}\sqrt{1+8m}\ .$$

Учитывая, что в практических приложениях используются сообщения с $m \ge 64$, можно записать следующее выражение для оценки верхней границы n:

$$n \le \left\lfloor \sqrt{2m} \right\rfloor.$$

Таким образом, сложность смещения ключа Y до значения $\widetilde{Y} = 2^{-2\left[\sqrt{2m}\right]}Y$ по сравнению со сложностью последующей оценки сообщения ничтожно мала, и ее можно не учитывать. Сложность оценки сообщения и атаки в целом:

$$S_{KM} \approx S_M = \left[2^{m-1}\widetilde{Y}\right] \approx 2^{m-2\sqrt{2m}-2},$$

или

$$\widetilde{s}(k,m) = k \cdot 2^{m-2\sqrt{2m}-2} = k \cdot e^{\ln(2)\left(m-2\sqrt{2m}-2\right)} = O\left(k \cdot e^{\ln(2)\left(m-2\sqrt{2m}\right)}\right). \qquad (7)$$

Эффективность пошагового смещения открытого ключа по сравнению с последовательным можно оценить как:

$$\frac{s(k,m)}{\widetilde{s}(k,m)} = \frac{\sqrt{2k}\left(2^{m/2}\right)}{k2^{m-2\sqrt{2m}-2}} = \sqrt{\frac{2}{k}}\left(2^{2\sqrt{2m}-m/2+2}\right) = O\left(\frac{1}{\sqrt{k}} \cdot e^{\ln(2)\left(\sqrt{2m}-m/2\right)}\right). \qquad (8)$$

Для $k = 1$, уже при $m > 41$ бит отношение (8) меньше единицы и, таким образом, пошаговое смещение открытого ключа Y оказывается менее эффективным.

Оценка стойкости криптосистемы, основанная на анализе сложности решения обратной задачи хаотической динамики, предполагает отсутствие более эффективных методов определения ее секретных параметров Q, P, N и, соответственно, восстановления открытого текста. Однако в предложенном выше варианте криптосистемы в распоряжении криптоаналитика оказывается достаточно инфор-

мации о секретных системных параметрах для проведения более эффективных атак, основанных на определении порядка N отображения и последующем нахождении Q и P, например, с использованием свойств неустойчивых неподвижных точек хаотических отображений.

Криптоанализ с использованием неустойчивых неподвижных точек

Для отображения $T_N(\ )$ значения X являются неустойчивыми неподвижными точками по определению, а Y и все значения шифротекста C являются неустойчивыми неподвижными точками вследствие выполнения следующих равенств:

$$T_N(Y) = T_N(T_P(X)) = T_P(T_N(X)) = T_P(X) = Y,$$
$$T_N(C) = T_N(T_M(Y)) = T_M(T_N(Y)) = T_M(Y) = C.$$

Решая уравнение $Y = T_N(Y)$, можно оценить порядок отображения:

$$N_i^Y = \frac{\pm\arccos(\cos(\pi Y)) + 2\pi i}{\pi Y} = \pm\frac{\arccos(\cos(\pi Y))}{\pi Y} + \frac{2}{Y}i = \\ = \pm\frac{Y}{Y} + \frac{2}{Y}i = \pm 1 + \frac{2}{Y}i,\ i = 0,1,.... \tag{9}$$

Емкость множества оценок равна $V_N = 2\cdot i_{\max} = [N_{\max}\cdot Y]$. Таким образом, определение целочисленного значения N из выражения (9) является более сложной задачей по сравнению с криптоанализом, использующим выражение (4), вследствие того, что $N > M_{\max}$. Решение уравнения $C = T_N(C)$ также дает оценки:

$$N_j^C = \frac{\pm\arccos(\cos(\pi C)) + 2\pi j}{\pi C} = \pm\frac{\arccos(\cos(\pi C))}{\pi C} + \frac{2}{C}j = \\ = \pm\frac{C}{C} + \frac{2}{C}j = \pm 1 + \frac{2}{C}j,\ j = 0,1,.... \tag{10}$$

Емкость их множества равна $V_N = 2\cdot j_{\max} = [N_{\max}\cdot C]$. Если криптоаналитик получит значение C близкое к началу координат, то это позволит значительно уменьшить емкость V_N, либо вообще исключить неоднозначность в (10). Кроме того множества $\{N\}$, получаемые из выражений (9) и (10), имеют пересечение $\{N_i^Y\}_{i=1}^{i_{\max}} \cap \{N_j^C\}_{j=1}^{j_{\max}}$, единственный элемент которого — искомое натуральное значение N. Соответственно попарно разделив левые и правые части выражений (9) и (10), получим:

$$\frac{N_i^Y \pm 1}{N_j^C \pm 1} = \frac{C\cdot i}{Y\cdot j},\ i = 0,1,...,\ j = 0,1,....$$

Для пересечения $\{M_i^Y\}_{i=1}^{i_{\max}} \cap \{M_j^C\}_{j=1}^{j_{\max}}$:

$$\frac{i}{j} = \frac{Y}{C}. \qquad (11)$$

Таким образом, задача определения N с использованием соотношения (11) оказывается достаточно просто решаемой. Сложность криптоанализа для предложенного варианта криптосистемы сводится к факторизации N на простые сомножители P и Q, и соизмерима со сложностью криптоанализа RSA.

Вообще говоря, при формировании ключей числа P и Q можно выбирать не только простыми, но и натуральными. Однако в этом случае неустойчивая неподвижная точка X может принадлежать орбите более низкого порядка, что позволит определить личный ключ усилиями, соизмеримыми с ее порядком.

Для устранения возможности определения N с использованием (11) необходимо модифицировать выбор ключей в криптосистеме следующим образом. Значение N выбираем простым, выполняя условие $N > M_{\max}$. Это требование позволяет исключить из группы неустойчивых неподвижных точек отображения $T_N(\ )$ неустойчивые неподвижные точки отображений меньшего порядка. В качестве параметра Q следует выбирать любое натуральное значение близкое к $\sqrt{N}$. Тогда параметр $P = N/Q$ будет вещественным значением. Такой выбор параметров не нарушает свойство (1), которое выполняется для кусочно-линейного отображения не только при целых значениях порядка, но и в случае, если порядок внутреннего отображения $T_P(X)$ задается вещественным значением:

$$T_Q(T_P(X)) = \frac{1}{\pi}\arccos(\cos(Q\pi(\frac{1}{\pi}\arccos(\cos(P\pi X))))) = \frac{1}{\pi}\arccos(\cos(Q\pi(-PX + 2n))),$$

где n целое, такое что $-1 < (-PX + 2n) < 1$. Если Q — целое, то:

$$T_Q(T_P(X)) = \frac{1}{\pi}\arccos(\cos(-\pi QPX + 2\pi Qn))) = \frac{1}{\pi}\arccos(\cos(\pi QPX))) = T_{Q\cdot P}(X),$$

так как слагаемое $2\pi Qn$ кратно периоду функции $\cos(\ )$. Если Q — вещественное, то слагаемое $2\pi Qn$ нельзя отбрасывать, и отображение имеет сложную структуру. Очевидно, что для рассматриваемого случая свойство (2) не выполняется.

Для такого выбора ключей точки Y и C не будут являться неустойчивыми неподвижными точками отображения $T_N(\ )$. Следовательно, можно утверждать, что сложность криптоанализа в этом случае определяется сложностью решения обратной задачи хаотической динамики.

Выводы

В работе предложен подход к решению задачи обеспечения защиты информации в компьютерных системах и сетях, основанный на использовании достиже-

ний хаотической динамики, который открывает новые возможности эффективного ее решения. Анализ показал, что эффективность предложенного подхода определяется сложностью решения обратной задачи хаотической динамики, которая имеет экспоненциальную зависимость от длины m блока открытого текста (ключа). Даже при анализе одного сообщения подход обеспечивает стойкость не меньшую, чем наилучшие в настоящее время криптосистемы с открытым ключом, использующие преобразования на эллиптических кривых [17]. При этом стойкость основана не на «вычислительной сложности» криптоанализа теоретико-числовых алгоритмов, а на неоднозначности обращения хаотического отображения (оценки порядка) в случае незнания личного ключа и его статистических свойствах.

1. *Птицин Н.И.* Приложение теории детерминированного хаоса в криптографии. — М.: МГТУ, 2002. — 79 с. ил.

2. *Kocarev L.* Chaos-Based Cryptography: A Brief Overview // IEEE Circuits and Systems Magazine. — 2001. — Vol. 1. — P. 6–21.

3. *Kocarev L., Tasev Z.* Public-Key Encryption Based on Chebyshev Maps // Proc. IEEE Symp. on Circuits and Systems (ISCAS-2003). — 2003. — Vol. 3. — P. 28–31.

4. *Masuda N., Aihara K.* Cryptosystem With Discretized Chaotic Maps // IEEE Transactions on Circuits and Systems 1: Fundamental Theory and Applications. — 2002. — Vol. 49. — N 1. — P. 28–39.

5. *Kotulski Z., et. al.* Application of Discrete Chaotic Dynamical Systems in Cryptography — DCC Method // International Journal Bifurcation and Chaos. — 1999. — Vol. 9. — P. 1121–1135.

6. *Diffie W., Hellman M.* New Directions in Cryptography // IEEE Transactions on Information Theory. — 1976. — Vol. 22. — P. 644–654.

7. *Rivest R., Shamir A., Adleman L. A* Method for Obtaining Digital Signatures and Public Key Cryptosystem // ACM Communications. — 1978. — Vol. 21. — P. 120–126.

8. Федеральный стандарт обработки информации FIPS PUB 186 // NIST USA. — 1996.

9. *ElGamal T.* A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory. — 1985. — Vol. 31. — P. 469–472.

10. *Schnorr C.* Efficient Identification and a Signatures for Smart Card // Journal of Cryptology. — 1991. — N. 3.

11. *Koblitz N.* Elliptic Curve Cryptography // Math. Comput. — 1987. — Vol. 48. — P. 203–209.

12. *Cowie J., et al.* A World Wide Number Field Sieve Factoring Record: On to 512 Bits // Proc. ASIACRYPT'96. —1996, Nov.

13. *Odiyzko A.* The Future of Integer Factorization // CryptoBytes. — 1995, Sum.

14. *Wiener M.* Cryptanalysis of Short RSA Secret Exponents // IEEE Transactions on Information Theory. — 1990. — Vol. IT-36.

15. *Kotulski Z., et. al.* On Constructive Approach to Chaotic Pseudorandom Number Generator // RCMCIS. — 2002.

16. *Шустер Г.* Детерминированный хаос: Пер. с англ. — М.: Мир, 1985. — 255 с. ил.

17. *Столингс В.* Криптография и защита сетей: принципы и практика. — 2-е изд.: Пер. с англ. — М.: Издательский дом «Вильямс», 2001. — 672 с. ил. — Парал. тит. англ.

Поступила в редакцию 20.02.2006