разного уровня сложности, требущие для восстановления неизвестного входа дополнительную информацию разного рода. Рассмотрены конструкции таких систем, обладающих различной степенью обратимости: идентифицируемые, обратимые, обратимые на нескольких траекториях. Показано, что при использовании множества траекторий максимально широкий класс динамических система становится идентифицируемым. Предлагается соответствующая схема передачи и восстановления сообщения, в которой передаваемый сигнал используется для синтеза дополнительных выходов системы, после чего восстановление входа системы осуществляется с использованием сигнала, заданного на множестве траекторий.

При реализации таких систем на компьютере, например, как криптографических систем, возникает необходимость перехода к дискретным аналогам непрерывных динамических систем. Такие аналоги предложены в виде конечных автоматов, описываемых системами уравнений над конечными полями или кольцами. При этом разные типы обратимости получают естественную теоретико-автоматную интерпретацию. Введено понятие k-кратного без потери информации автомата (k-БПИ), которое аналогично понятию обратимости на нескольких траекториях. Для ряда систем (Лоренца, Рёсслера, Чуа) введены их автоматные аналоги и на их основе предложены поточные криптоалгоритмы. В рамках теории экспериментов с автоматами выполнена формализация атак на такие криптосистемы и доказана NP-полнота задачи о распознавании контрольного эксперимента для k-БПИ-автоматов, лежащая в основе такой формализации.

Использование методики нескольких траекторий для обратимых нелинейных динамических систем и их автоматных аналогов, задаваемых уравнениями над конечными кольцами и полями, позволяет разработать метод управления размерностью пространства состояний, отличный от метода, предложенного в работе [3]. При этом возникает система с переменной структурой, в которой к ключевым параметрам (элементам кольца или поля) добавляется структурный ключ, с помощью которого осуществляется выбор количества траекторий передающей системы.

ЛИТЕРАТУРА

1. *Ковалев А. М., Щербак В. Ф.* Управляемость, наблюдаемость, идентифицируемость динамических систем. Киев: Наук. думка, 1993. 285 с.
2. *Feldmann U., Hasler M., Schwarz W.* Communication by chaotic signals: the inverse system approach // Int. J. Circ. Theory Appl. 1996. V. 24. P. 551–579.
3. *Ковалев А. М., Козловский В. А., Щербак В. Ф.* Обратимые динамические системы с переменной размерностью фазового пространства в задачах криптографического преобразования информации // Прикладная дискретная математика. 2008. № 2(2). С. 39–44.

УДК 519.7

О ПОТОЧНЫХ И АВТОМАТНЫХ ШИФРСИСТЕМАХ

И. В. Панкратов

Ранее в работе автора [1] были определены понятия поточной шифрсистемы и самосинхронизирующихся с задержкой поточной и регистровой шифрсистем и было показано, что последними исчерпываются все поточные самосинхронизирующиеся системы, у которых проекции генератора ключевого потока являются сильносвязными автоматами. В настоящей работе определяются ещё и понятия автоматной и самосинхронизирующейся с задержкой автоматной шифрсистем и устанавливается, что реги-

стровыми шифрсистемами исчерпываются также и автоматные самосинхронизирующиеся системы с сильносвязными проекциями автомата расшифрования (теорема 3). Более того, установлено, что классы поточных и автоматных шифрсистем функционально эквивалентны (теорема 1), а именно: для каждой системы любого из этих классов существует система в другом классе, которая задаёт то же семейство последовательностных шифров, что и первая. Наконец, как альтернатива конструктивному определению понятия поточной самосинхронизирующейся шифрсистемы в [1] здесь даётся дескриптивное определение этого понятия и показывается равносильность обоих определений (теорема 2).

Условимся конечный автомат (Мили) с входным алфавитом X, выходным алфавитом Y, множеством состояний Q и функциями переходов и выходов $\psi\colon Q \times X \to Q$ и $\varphi\colon Q \times X \to Y$ соответственно обозначать набором $A =< X, Q, Y, \psi, \varphi >$. В нём функции ψ и φ, определённые на $Q \times X$, считаются определёнными (индукцией по длине входного слова) и на $Q \times X^*$. Последовательность выходных символов, которую автомат вырабатывает из начального состояния $q \in Q$ под действием входного слова α, обозначается $\bar{\varphi}_q(\alpha)$. В автомате Мура A, где функция $\varphi(q, x)$ зависит от аргумента x фиктивно и является фактически функцией из Q в Y, иногда вместо $\varphi(q, x)$ пишем $\varphi(q)$.

Для автомата с двумя входами $A =< X \times K, Q, Y, \psi, \varphi >$ и произвольного $k \in K$ вводятся функции $\psi_k(q, x) = \psi(q, (x, k))$, $\varphi_k(q, x) = \varphi(q, (x, k))$ и автомат $A_k =< X, Q, Y, \psi_k, \varphi_k >$, называемый *проекцией автомата A на вход X при данном $k \in K$*.

Определение 1. *Последовательностным шифром* называется набор из пяти объектов $S =< X, Y, K, f, f^{-1} >$, где X, Y и K — конечные множества, называемые соответственно *входным алфавитом*, *выходным алфавитом* и *ключевым пространством*, f и f^{-1} — функции, $f\colon X^* \times K \to Y^*$, $f^{-1}\colon Y^* \times K \to X^*$, называемые функциями соответственно *шифрования* и *расшифрования* и связанные отношением обратимости

$$\forall x \in X^* \forall y \in Y^* \forall k \in K [f(x, k) = y \Rightarrow f^{-1}(y, k) = x].$$

Определение 2 [1]. Назовём *поточной шифрсистемой* набор из шести объектов $\Sigma_S =< X, Y, K, G, e, d >$, где $G =< Y \times K, Q, \Gamma, \psi, \varphi >$ — конечный автомат, называемый *генератором ключевого потока* (*ГКП*), такой, что любая его проекция G_k есть автомат Мура, $e\colon X \times \Gamma \to Y$, $d\colon Y \times \Gamma \to X$ — правила шифрования и расшифрования одного символа открытого текста (сообщения) с помощью одного символа ключевого потока (гаммы), связанные отношением обратимости:

$$\forall \gamma \in \Gamma \forall x \in X \forall y \in Y [e(x, \gamma) = y \Rightarrow d(y, \gamma) = x].$$

Определим в Σ_S функции $E\colon Q \times X^* \times K \to Y^*$ и $D\colon Q \times Y^* \times K \to X^*$ — соответственно правила шифрования и расшифрования сообщений по ключу и начальному состоянию — по следующим формулам:

$$E(q_0, \Lambda, k) = \Lambda,$$

$$E(q_0, x_0 x_1 \dots x_{n-1}, k) = y_0 y_1 \dots y_{n-1}, \text{ где } \begin{cases} \gamma_t = \varphi_k(q_t), \\ y_t = e(x_t, \gamma_t), \quad t = 0, 1, \dots, n-1; \\ q_{t+1} = \psi_k(q_t, y_t), \end{cases}$$

$$D(q_0, \Lambda, k) = \Lambda,$$

$$D(q_0, y_0 y_1 \dots y_{n-1}, k) = x_0 x_1 \dots x_{n-1}, \text{ где } \begin{cases} \gamma_t = \varphi_k(q_t), \\ x_t = d(y_t, \gamma_t), \quad t = 0, 1, \dots, n-1. \\ q_{t+1} = \psi_k(q_t, y_t), \end{cases}$$

По определению функций E и D легко проверить, что при любых G, $q \in Q$, e и d, где e и d связаны отношением обратимости, пятерка $S_q(S) = < X, Y, K, E_q, D_q >$, где E_q и D_q — функции соответственно E и D с фиксированным значением первого аргумента $q \in Q$, будет последовательностным шифром. Множество $\{S_q(S) \mid q \in Q\}$ всех таких шифров называется далее *семейством последовательностных шифров, задаваемых шифрсистемой* Σ_S.

Определение 3. Назовём *автоматной шифрсистемой* пятерку объектов $\Sigma_A = < X, Y, K, A^e, A^d >$, где $A^e = < X \times K, Q, Y, \psi, \varphi >$ и $A^d = < Y \times K, Q^*, X, \psi^*, \varphi^* >$ суть конечные приведённые автоматы, называемые *автоматами шифрования* и *расшифрования* соответственно, если для любого состояния $q \in Q$ найдется такое состояние $q^* \in Q^*$, что пятерка $S_{qq^*}(A) = < X, Y, K, \bar{\varphi}_q, \bar{\varphi}^*_{q^*} >$ будет последовательностным шифром.

Множество $\{S_{qq^*}(A) \mid q \in Q\}$ называется далее *семейством последовательностных шифров, задаваемых шифрсистемой* Σ_A.

Две шифрсистемы (поточные или автоматные) называются *эквивалентными*, если они задают одно и то же семейство последовательностных шифров. Два класса шифрсистем (поточных или автоматных) *равносильны*, если каждая шифрсистема любого из них эквивалентна некоторой шифрсистеме другого.

Теорема 1. Классы поточных и автоматных шифрсистем равносильны.

Определение 4 [1]. Назовём автомат $A =< X, Q, Y, \psi, \varphi >$ *самосинхронизирующимся с задержкой* τ, если выполняется условие

$$\forall q \in Q \forall x, x' \in X^* \forall \tilde{x} \in X^\tau \forall u \in X^* [\bar{\varphi}(\psi(q, x\tilde{x}), u) = \bar{\varphi}(\psi(q, x'\tilde{x}), u)].$$

Определение 5. Последовательностный шифр $S = < X, Y, K, f, f^{-1} >$ называется *самосинхронизирующимся с задержкой* τ, если выполняются следующие условия:

1) $\forall y \in Y^* \forall k \in K \, |f^{-1}(y, k)| = |y|$;
2) для любых y_1, y_3, y_1' в Y^*, y_2 в Y^τ, x_1, x_3, x_1', x_3' в X^*, x_2, x_2' в X^τ и $k \in K$, таких, что $|x_3| = |x_3'|$, $f^{-1}(y_1 y_2 y_3, k) = x_1 x_2 x_3$ и $f^{-1}(y_1' y_2 y_3, k) = x_1' x_2' x_3'$, имеет место $x_3 = x_3'$.

Определение 6 (конструктивное) [1]. Назовём поточную шифрсистему $\Sigma_S = < X, K, Y, G, e, d >$ *самосинхронизирующейся с задержкой* τ, если при любом ключе $k \in K$ проекция G_k автомата G является самосинхронизирующимся автоматом с задержкой τ.

Определение 7 (дескриптивное). Назовём поточную шифрсистему *самосинхронизирующейся с задержкой* τ , если все задаваемые ею последовательностные шифры являются самосинхронизирующимися с задержкой τ.

Теорема 2. Дескриптивное и конструктивное определения самосинхронизирующейся поточной шифрсистемы эквивалентны.

Определение 8 [1]. Назовём автомат Мура $R = < Y, Y^\tau, \Gamma, \sigma, \varphi >$ *регистром сдвига длиной* τ, если его функция переходов σ есть функция сдвига, определяемая по формуле

$$\forall y_1 y_2 \dots y_\tau \in Y^\tau \forall y \in Y [\sigma(y_1 y_2 \dots y_\tau, y) = y_2 \dots y_\tau y].$$

Определение 9 [1]. Назовём *регистром сдвига длиной* τ *с ключом* такой автомат Мили с двумя входами $R = < Y \times K, Y^\tau, \Gamma, \sigma', \varphi >$, что для любого значения $k \in K$ его проекция $R_k = < Y, Y^\tau, \Gamma, \sigma'_k, \varphi_k >$ на вход Y есть регистр сдвига длиной τ.

Определение 10 [1]. Назовём поточную шифрсистему $\Sigma_R = < X, K, Y, R, \varepsilon, \delta >$ *регистровой*, если её ГКП R есть регистр сдвига с ключом. Длина регистра R называется размерностью шифрсистемы.

Регистровая шифрсистема размерностью τ является самосинхронизирующейся с задержкой τ по конструктивному определению.

Определение 11. Назовём автоматную шифрсистему $\Sigma_A = < X, Y, K, A^e, A^d >$ *самосинхронизирующейся с задержкой* τ, если таковой является проекция A^d_k автомата A^d для любого $k \in K$:

$$\forall q_0^* \in Q^* \forall y, y' \in Y^* \forall \tilde{y} \in Y^\tau \forall u \in Y^* [\bar{\varphi}^*_k(\psi^*_k(q_0^*, y\tilde{y}), u) = \bar{\varphi}^*_k(\psi^*_k(q_0^*, y'\tilde{y}), u)].$$

Говорят, что некоторая шифрсистема *неотличима от шифрсистемы* Σ, если задаваемые ею последовательностные шифры задаются системой Σ.

Теорема 3. Любая самосинхронизирующаяся с задержкой τ автоматная шифрсистема $\Sigma_A = < X, K, Y, A^e, A^d >$, у которой все проекции A^d_k автомата расшифрования A^d суть сильно связные автоматы, неотличима от некоторой регистровой шифрсистемы $\Sigma_R = < X, K, Y, R, \varepsilon, \delta >$ размерности τ.

ЛИТЕРАТУРА

1. *Панкратов И. В.* К определению понятия самосинхронизирующегося поточного шифра // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 114–117.

УДК 519.7

ОЦЕНКА ПОКАЗАТЕЛЯ 2-ТРАНЗИТИВНОСТИ ОБОБЩЁННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ФЕЙСТЕЛЯ[1]

М. А. Пудовкина

Различные обобщения алгоритма шифрования Фейстеля рассмотрены в работах [1 – 6] и др. Некоторые из них являются обобщением конструкций блочных алгоритмов CAST, IDEA, MARS, SKIPJACK и др. В данной работе вводится единая математическая модель, описывающая единым образом разнообразные известные обобщения алгоритма шифрования Фейстеля.

Пусть натуральное $n \geqslant 2$, V_m — множество всех m-мерных двоичных векторов над полем $GF(2)$; $X^* = X \backslash \{0\}$; $P(X)$ — множество всех отображений из X в X; $S(X)$ — множество всех подстановок на X; $\oplus$ — операция покоординатного сложения векторов из V_m; o — нулевое отображение, т. е. $\alpha^o = \mathbf{0}$ для любого $\alpha \in V_m$; e — тождественное отображение; $P(V_m)^0 = \{o\}$, $S(V_m)^{[0]} = \{e\}$, $S(V_m)^{[1]} = S(V_m)$, $\Upsilon_n = \{\upsilon : \{\overline{1,n}\} \to \{0,1\} | \upsilon(1) = 1\}$.

[1]Работа выполнена при поддержке гранта Президента РФ НШ № 4.2008.10.