МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

О ПОТОЧНЫХ И АВТОМАТНЫХ ШИФРСИСТЕМАХ С СИММЕТРИЧНЫМ КЛЮЧОМ[1]

И. В. Панкратов

Томский государственный университет, г. Томск, Россия

E-mail: ivan.pankr@gmail.com

Рассматриваются симметричные поточные и автоматные шифрсистемы. Показывается неотличимость поточных шифрсистем, у которых неотличимы генераторы ключевого потока; определяются понятия последовательностного шифра, автоматной и самосинхронизирующейся с задержкой автоматной шифрсистем; показывается инъективность функции выходов автомата шифрования в автоматной шифрсистеме при любой фиксации состояния автомата и ключа шифрсистемы; устанавливается функциональная эквивалентность классов поточных и автоматных шифрсистем, а именно: для каждой системы любого из этих классов существует система в другом классе, которая задаёт то же семейство последовательностных шифров, что и первая; как альтернатива конструктивному определению понятия поточной самосинхронизирующейся шифрсистемы даётся дескриптивное определение этого понятия и устанавливается равносильность обоих определений; показывается, что регистровыми шифрсистемами исчерпываются все автоматные самосинхронизирующиеся системы с сильносвязными проекциями автомата шифрования.

Ключевые слова: *поточная шифрсистема, автоматная шифрсистема, последовательностный шифр, самосинхронизирующаяся шифрсистема, генератор ключевого потока, регистровая шифрсистема.*

Введение

В данной работе все рассматриваемые шифрсистемы и шифры предполагаются симметричными, а автоматы — конечными. Продолжаются исследования, начатые автором в [1], где 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. Показывается неотличимость поточных шифрсистем, имеющих неотличимые генераторы ключевого потока (теорема 1); определяются понятия последовательностного шифра, автоматной и самосинхронизирующейся с задержкой автоматной шифрсистем; доказывается, что функция выходов автомата шифрования в автоматной шифрсистеме инъективна при любой фиксации состояния автомата и ключа шифрсистемы (теорема 2); устанавливается функциональная эквивалентность классов поточных и автоматных шифрсистем (теорема 3), а именно: для каждой системы любого из этих

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы. Результаты работы докладывались на Международной конференции с элементами научной школы для молодёжи, г. Омск, 7–12 сентября 2009 г.

классов существует система в другом классе, которая задаёт то же семейство последовательностных шифров, что и первая; как альтернатива конструктивному определению в [1] понятия поточной самосинхронизирующейся шифрсистемы (в терминах самосинхронизирующихся проекций генератора ключевого потока) здесь даётся ещё и дескриптивное определение этого понятия (в терминах задаваемых самосинхронизирующихся последовательностных шифров) и показывается равносильность обоих определений (теорема 4); наконец, устанавливается, что регистровыми шифрсистемами исчерпываются также и автоматные самосинхронизирующиеся системы с сильносвязными проекциями автомата шифрования (теорема 6). Формулировку теорем 3, 4, 6 (без доказательства) можно найти в тезисах работы [2].

Все теоретико-автоматные понятия и обозначения, используемые в статье, заимствуются из [3]. 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 обозначается 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 $\bar{\varphi}(q, \alpha)$ или $\bar{\varphi}_q(\alpha)$. 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 $\varphi(q)$.

В автомате $A = <X \times K, Q, Y, \psi, \varphi>$ с двумя входами X называется алфавитом сообщений, K — множеством, или пространством, ключей и X^* — множеством сообщений. В нём для произвольного ключа $k \in K$ вводятся функции $\psi_k(q, x) = \psi(q, (x, k))$ и $\varphi_k(q, x) = \varphi(q, (x, k))$ соответственно переходов и выходов на ключе k и автомат $A_k = <X, Q, Y, \psi_k, \varphi_k>$, называемый *проекцией автомата A на вход X при данном ключе $k \in K$*. Наконец, понятие последовательностного шифра определяется следующим образом.

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

$$\forall \alpha \in X^* \forall \beta \in Y^* \forall k \in K [f(\alpha, k) = \beta \Rightarrow g(\beta, k) = \alpha].$$

Последовательностные шифры с общей функцией шифрования считаются равными.

1. Поточные шифрсистемы

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

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

Введём для Σ_S функции $\bar{e}\colon Q \times X^* \times K \to Y^*$ и $\bar{d}\colon Q \times Y^* \times K \to X^*$, называемые *алгоритмами* соответственно *шифрования* и *расшифрования сообщений*, которые по

ключу k и начальному состоянию q_0 определяются по следующим формулам:

$$\bar{e}(q_0, \Lambda, k) = \Lambda,$$

$$\bar{e}(q_0, x_0x_1 \dots x_{n-1}, k) = y_0y_1 \dots y_{n-1}, \text{ где } \begin{cases} \gamma_t = \varphi_k(q_t), \\ y_t = e(x_t, \gamma_t), \\ q_{t+1} = \psi_k(q_t, y_t), \end{cases} \quad t = 0, 1, \dots, n-1,$$

$$\bar{d}(q_0, \Lambda, k) = \Lambda,$$

$$\bar{d}(q_0, y_0y_1 \dots y_{n-1}, k) = x_0x_1 \dots x_{n-1}, \text{ где } \begin{cases} \gamma_t = \varphi_k(q_t), \\ x_t = d(y_t, \gamma_t), \\ q_{t+1} = \psi_k(q_t, y_t), \end{cases} \quad t = 0, 1, \dots, n-1.$$

Эти уравнения проиллюстрированы схемами на рис. 1 и 2, где D обозначает элемент задержки на единицу дискретного времени. В них последовательности $q_0q_1 \dots$ и $\gamma_0\gamma_1 \dots$ называются соответственно последовательностью состояний и ключевым потоком, или гаммой, вырабатываемыми в ГКП G из начального состояния q_0 при заданном ключе k под воздействием входного слова $y_0y_1 \dots$

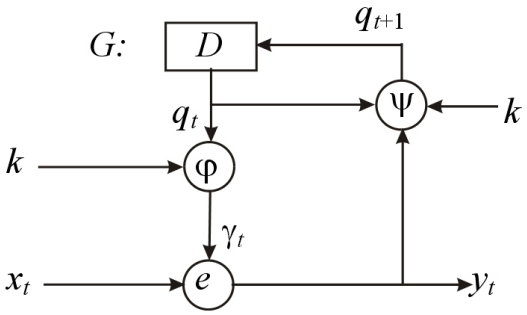

Рис. 1. Схема алгоритма шифрования в поточной шифрсистеме

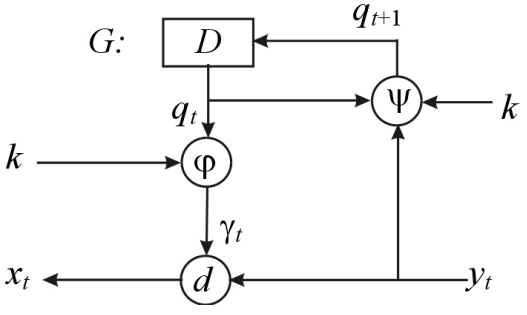

Рис. 2. Схема алгоритма расшифрования в поточной шифрсистеме

По определению функций $\bar{e}$ и $\bar{d}$ легко проверить, что при любых G, $q \in Q$, e и d, где e и d связаны отношением обратимости, пятерка $S_q(\Sigma_S) = <X, Y, K, \bar{e}_q, \bar{d}_q>$, где $\bar{e}_q \colon X^* \times K \to Y^*$, $\bar{d}_q \colon Y^* \times K \to X^*$ и $\bar{e}_q(\alpha, k) = e(q, \alpha, k)$, $\bar{d}_q(\beta, k) = d(q, \beta, k)$ для всех $k \in K$, $\alpha \in X^*$ и $\beta \in Y^*$, будет последовательностным шифром. Множество

$S(\Sigma_S) = \{S_q(\Sigma_S) \mid q \in Q\}$ всех таких шифров называется далее *семейством последовательностных шифров, задаваемых шифрсистемой* Σ_S.

Возможны различные варианты использования поточной шифрсистемы в зависимости от выбора начального состояния q_0 её ГКП: 1) q_0 фиксировано и заранее известно; 2) q_0 вычисляется открытым способом по ключу; 3) q_0 вычисляется как некая случайная величина и каким-то образом (открыто или закрыто) передается корреспонденту. В [1] показан вариант вероятностной самосинхронизирующейся поточной шифрсистемы, в котором начальное состояние генерируется случайно и в открытом виде передается корреспонденту вместе с криптограммой. В общем случае начальное состояние является вероятностной функцией от ключа.

Поточную шифрсистему $\Sigma_S = <X, Y, K, G, e, d>$ будем называть *неотличимой* [1] от поточной шифрсистемы $\Sigma'_S = <X, Y, K, G', e', d'>$, где $G = <Y \times K, Q, \Gamma, \psi, \varphi>$ и $G' = <Y \times K, Q', \Gamma', \psi', \varphi'>$, если выполняется следующее соотношение:

$$\forall k \in K \forall q \in Q \exists q' \in Q' \forall \alpha \in X^* [\bar{e}(q, \alpha, k) = \bar{e}'(q', \alpha, k)].$$

Отметим, что неотличимость двух поточных шифрсистем друг от друга не влечёт равенства семейств задаваемых ими последовательностных шифров. Причина в порядке кванторов. Содержательно неотличимость гласит, что для любого ключа и для любого начального состояния первой шифрсистемы найдется такое начальное состояние второй шифрсистемы, что соответствующие алгоритмы шифрования будут совпадать. Однако при этом возможно, что при разных ключах одному и тому же состоянию первой шифрсистемы будут соответствовать разные состояния второй шифрсистемы, то есть может вообще не быть таких начальных состояний разных шифрсистем, в которых шифрсистемы задают одинаковые последовательностные шифры.

Будем говорить, что ГКП $G = <Y \times K, Q, \Gamma, \psi, \varphi>$ *неотличим* от ГКП $G' = <Y \times K, Q', \Gamma, \psi', \varphi'>$, если для любого ключа $k \in K$ его проекция G_k на вход Y сильно неотличима [3] от аналогичной проекции G'_k, т. е. каждое состояние в G_k неотличимо от некоторого состояния в G'_k.

Теорема 1. Пусть $\Sigma_S = <X, Y, K, G, e, d>$ и $\Sigma'_S = <X, Y, K, G', e, d>$ — две шифрсистемы с разными ГКП G и G'. Тогда если G неотличим от G', то и Σ_S неотличима от Σ'_S.

Доказательство. Пусть $G = <Y \times K, Q, \Gamma, \psi, \varphi>$, $G' = <Y \times K, Q', \Gamma, \psi', \varphi'>$. Возьмём произвольные $k \in K$, $q_0 \in Q$, $\alpha = x_0 x_1 \dots x_{n-1} \in X^*$ и состояние $q'_0 \in Q'$, неотличимое от $q_0 \in Q$.

Будем иметь

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

$$\bar{e}'(q'_0, x_0 x_1 \dots x_{n-1}, k) = y'_0 y'_1 \dots y'_{n-1}, \text{ где } \begin{cases} \gamma'_t = \varphi'_k(q'_t), \\ y'_t = e(x_t, \gamma'_t), \\ q'_{t+1} = \psi'_k(q'_t, y'_t), \end{cases} \quad t = 0, 1, \dots, n-1.$$

Индукцией по t убедимся в равенстве $y_t = y'_t$ для каждого $t = 0, 1, \dots, n-1$.

База индукции: $t = 0$. Имеем: $\gamma_0 = \varphi_k(q_0) = \varphi'_k(q'_0) = \gamma'_0$, $y_0 = e(x_0, \gamma_0) = e(x_0, \gamma'_0) = y'_0$.

Предположение индукции. Предположим, что $y_0y_1\dots y_{t-1} = y'_0y'_1\dots y'_{t-1}$ для некоторого $t \geqslant 1$.

Шаг индукции. Ввиду неотличимости состояний $\psi_k(q_0, y_0y_1\dots y_{t-1})$ и $\psi'_k(q'_0, y_0y_1\dots y_{t-1})$, следующей из неотличимости q_0 и q'_0, можно записать $\gamma_t = \varphi_k(q_t) = \varphi_k(\psi_k(q_{t-1}, y_{t-1})) = \varphi_k(\psi_k(q_0, y_0y_1\dots y_{t-1})) = \varphi'_k(\psi'_k(q'_0, y_0y_1\dots y_{t-1})) = \varphi'_k(\psi'_k(q'_0, y'_0y'_1\dots y'_{t-1})) = \varphi'_k(\psi'_k(q'_{t-1}, y'_{t-1})) = \varphi'_k(q'_t) = \gamma'_t$ и $y_t = e(x_t, \gamma_t) = e(x_t, \gamma'_t) = y'_t$.

Индуктивное заключение: $y_0y_1\dots y_{n-1} = y'_0y'_1\dots y'_{n-1}$.

Следовательно, $\bar{e}(q_0, \alpha, k) = \bar{e}'(q'_0, \alpha, k)$.

Ввиду произвольности $k \in K$, $q_0 \in Q$ и $\alpha \in X^*$ теорема доказана. ■

Таким образом, установлено, что при замене в шифрсистеме одного ГКП на другой, неотличимый от него, получится шифрсистема, неотличимая от исходной.

2. Автоматные шифрсистемы

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

$$\forall q \in Q \exists q^* \in Q^* \forall k \in K \forall \alpha \in X^* \forall \beta \in Y^* [\bar{\varphi}_q(\alpha, k) = \beta \Rightarrow \bar{\varphi}^*_{q^*}(\beta, k) = \alpha].$$

Определение 4. Множество $S(\Sigma_A) = \{S_{qq^*}(\Sigma_A) \mid q \in Q\}$ называется далее *семейством последовательностных шифров, задаваемых шифрсистемой* Σ_A.

Теорема 2. Функция выходов автомата шифрования автоматной шифрсистемы при фиксированных значениях состояния и ключа инъективна как функция одного аргумента — символа сообщений.

Доказательство. Пусть $\Sigma_A = <X, Y, K, E, D>$ есть автоматная шифрсистема с автоматами шифрования $E = <X \times K, Q, Y, \psi, \varphi>$ и расшифрования $D = <Y \times K, Q^*, X, \psi^*, \varphi^*>$. Докажем, что при любых фиксированных значениях состояния $q \in Q$ и ключа $k \in K$ функция $\varphi_{qk}(x) = \varphi(q, (x, k))$ инъективна.

Предположим противное: пусть для некоторых состояния $q \in Q$ и ключа $k \in K$

$$\exists x_1, x_2 \in X[(x_1 \neq x_2) \,\&\, (\varphi_{qk}(x_1) = \varphi_{qk}(x_2))].$$

Тогда по определению автоматной шифрсистемы Σ_A найдётся такое $q^* \in Q^*$, что для любых y_1 и y_2 в Y

$$\bar{\varphi}_q(x_1, k) = y_1 \Rightarrow \bar{\varphi}^*_{q^*}(y_1, k) = x_1,\ \bar{\varphi}_q(x_2, k) = y_2 \Rightarrow \bar{\varphi}^*_{q^*}(y_2, k) = x_2.$$

Здесь $\bar{\varphi}_q(x_1, k) = \varphi_{qk}(x_1)$ и $\bar{\varphi}_q(x_2, k) = \varphi_{qk}(x_2)$, поэтому $y_1 = y_2$ и, следовательно, $x_1 = x_2$, что не так. ■

Интересно отметить, что ещё 50 лет назад А. Д. Закревский [4] предложил использовать в качестве алгоритмов шифрования конечные автоматы с функцией выходов, инъективной в каждом состоянии. Теорема 2 говорит о том, что других автоматов, которые можно было бы использовать в этом качестве, не бывает.

3. Равносильность поточных и автоматных шифрсистем

Определение 5. Две шифрсистемы (поточные или автоматные) называются *эквивалентными*, если они задают одно и то же семейство последовательностных шифров (в предположении о равенстве шифров, отличающихся только функцией расшифрования). Два класса шифрсистем (поточных или автоматных) *равносильны*, если каждая шифрсистема любого из них эквивалентна некоторой шифрсистеме другого.

Теорема 3. Классы поточных и автоматных шифрсистем равносильны.

Доказательство. Докажем сначала, что каждая поточная шифрсистема эквивалентна некоторой автоматной шифрсистеме. Для этого возьмем произвольную поточную шифрсистему $\Sigma_S = <X, Y, K, G, e, d>$, где $G = <Y \times K, Q', \Gamma, \psi', \varphi'>$, и построим автоматную шифрсистему $\Sigma_A = <X, Y, K, E, D>$, где автоматы $E = <X \times K, Q, Y, \psi, \varphi>$ и $D = <Y \times K, Q^*, X, \psi^*, \varphi^*>$ определяются соотношениями

$$Q = Q^* = Q',$$

$$\psi(q,(x,k)) = \psi'(q, e(x, \varphi'(q,k)), k),\ \varphi(q,(x,k)) = e(x, \varphi'(q,k)),$$

$$\psi^*(q^*,(y,k)) = \psi'(q,y,k),\ \varphi^*(q^*,(y,k)) = d(y, \varphi'(q,k)).$$

Непосредственно проверяется, что

$$\forall q \in Q[(\bar{e}_q = \bar{\varphi}_q)\ \&\ (\bar{d}_q = \bar{\varphi}^*_q)].$$

Следовательно, $S_q(\Sigma_S) = S_{qq^*}(\Sigma_A)$ и $S(\Sigma_S) = S(\Sigma_A)$. Этим доказано, что поточная шифрсистема Σ_S эквивалентна автоматной шифрсистеме Σ_A.

Теперь докажем обратное, а именно: любая автоматная шифрсистема эквивалентна некоторой поточной шифрсистеме. Для этого возьмем произвольную автоматную шифрсистему $\Sigma_A = <X, Y, K, E, D>$, где $E = <X \times K, Q, Y, \psi, \varphi>$ и $D = <Y \times K, Q^*, X, \psi^*, \varphi^*>$, и построим поточную шифрсистему $\Sigma_S = <X, Y, K, G, e, d>$, где операции e, d и автомат $G = <Y \times K, Q', \Gamma, \psi', \varphi'>$ определяются соотношениями

$$Q' = Q,\ \Gamma = Q \times K,$$

$$e(x,\gamma) = e(x,(q,k)) = \varphi(q,(x,k)),\ d(y,\gamma) = d(y,(q,k)) = \varphi^{-1}_{qk}(y),$$

$$\psi'(q,(y,k)) = \psi(q,(d(y,(q,k)),k)) = \psi(q,(\varphi^{-1}_{qk}(y),k)),\ \varphi'(q,(y,k)) = (q,k),$$

где функция $\varphi^{-1}_{qk}(y)$ является обратной к функции $\varphi_{qk}(x)$. Она существует в силу инъективности последней по теореме 2.

Непосредственно проверяется, что

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

$$\forall q \in Q[\bar{\varphi}_q = \bar{e}_q\ \&\ \bar{\varphi}^*_q = \bar{d}_q].$$

Следовательно, $S_{qq^*}(\Sigma_A) = S_q(\Sigma_S)$ и $S(\Sigma_A) = S(\Sigma_S)$. Этим доказано, что автоматная шифрсистема Σ_A эквивалентна поточной шифрсистеме Σ_S. ■

Основная польза от этой теоремы заключается в том, что она позволяет к шифрсистемам одного класса применять результаты, полученные для шифрсистем другого класса, либо сконструировать шифрсистему по любой из этих двух схем и рассматривать её с обеих точек зрения.

4. Самосинхронизирующиеся поточные шифрсистемы

Определение 6 [1]. Назовём автомат $A = <X, Q, Y, \psi, \varphi>$ *самосинхронизирующимся с задержкой* τ, если выполняется условие

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

Содержательно это определение можно объяснить так: «В каком бы состоянии q автомат A ни находился, какую бы последовательность (α или α') входных символов в него ни подали, его выходная последовательность после подачи в него любого слова $\tilde{\alpha}$ длиной τ будет определяться только этим словом, последующей строкой входных символов ξ и, может быть, начальным состоянием q». Иными словами, происходит следующее: автомат строками α или α' переводится из состояния q в состояние $\psi(q, \alpha)$ или $\psi(q, \alpha')$ соответственно; затем строкой $\tilde{\alpha}$ длиной τ в состояние $\psi(\psi(q, \alpha), \tilde{\alpha}) = \psi(q, \alpha\tilde{\alpha})$ или $\psi(q, \alpha'\tilde{\alpha})$ соответственно; после этого он будет вести себя одинаково в обоих случаях (выдавая на входную последовательность ξ одну и ту же выходную), т. е. синхронизируется строкой $\tilde{\alpha}$.

Определение 7. Последовательностный шифр $S = <X, Y, K, f, g>$ называется *самосинхронизирующимся с задержкой* τ, если выполняются следующие условия:

1) $\forall \beta \in Y^* \forall k \in K\, |g(\beta, k)| = |\beta|$,
2) для любых β, ζ, β' в Y^*, $\tilde{\beta}$ в Y^τ, $\alpha, \xi, \alpha', \xi'$ в X^*, $\tilde{\alpha}, \tilde{\alpha'}$ в X^τ и $k \in K$, таких, что $|\xi| = |\xi'| = |\zeta|$, $g(\beta\tilde{\beta}\zeta, k) = \alpha\tilde{\alpha}\xi$ и $g(\beta'\tilde{\beta}\zeta, k) = \alpha'\tilde{\alpha'}\xi'$, имеет место $\xi = \xi'$.

Содержательный смысл этого понятия аналогичен предыдущему. Если произвольным образом исказить часть исходного шифртекста $\beta\tilde{\beta}\zeta$ (заменив β на β'), то при расшифровании искажения распространятся не далее чем на τ символов от последнего искаженного символа.

Определение 8 (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 9 (дескриптивное). Назовём поточную шифрсистему *самосинхронизирующейся с задержкой* τ, если все задаваемые ею последовательностные шифры являются самосинхронизирующимися с задержкой τ.

Будем предполагать далее, что в множестве Γ любой рассматриваемой поточной шифрсистемы Σ_S нет различных эквивалентных символов, т. е. таких γ и γ', что $\gamma \neq \gamma'$, но $\forall x \in X[e(x, \gamma) = e(x, \gamma')]$ и $\forall y \in Y[d(y, \gamma) = d(y, \gamma')]$. Ввиду возможности замены всех попарно эквивалентных символов гаммы одним из них без изменения результатов шифрования и расшифрования сообщений в системе данное предположение не приводит к потере общности рассмотрения.

Теорема 4. Дескриптивное и конструктивное определения самосинхронизирующейся поточной шифрсистемы (без эквивалентных символов гаммы) равносильны — определяют одно и то же множество шифрсистем.

Доказательство. Рассмотрим произвольную поточную шифрсистему $\Sigma_S = <X, Y, K, G, e, d>$ и её ГКП $G = <Y \times K, Q, \Gamma, \psi, \varphi>$. Требуется доказать равносильность следующих двух высказываний:

(Д) = «все последовательностные шифры, задаваемые системой Σ_S, являются самосинхронизирующимися с задержкой τ»;

(К) = «при любом ключе $k \in K$ проекция G_k автомата G является самосинхронизирующимся автоматом с задержкой τ».

Используем следующие обозначения:

$$\beta = y_{-n}y_{-n+1}\dots y_{-1};\ \beta' = y'_{-m}y'_{-m+1}\dots y'_{-1};\ \tilde{\beta} = y_0y_1\dots y_{\tau-1};\ \zeta = y_\tau y_{\tau+1}\dots y_{l-1};$$

$$\alpha = x_{-n}x_{-n+1}\dots x_{-1};\ \tilde{\alpha} = x_0x_1\dots x_{\tau-1};\ \alpha' = x'_{-m}x'_{-m+1}\dots x'_{-1};\tilde{\alpha'} = x'_0x'_1\dots x'_{\tau-1};$$

$$\xi = x_\tau x_{\tau+1}\dots x_{l-1};\ \xi' = x'_\tau x'_{\tau+1}\dots x'_{l-1},$$

где $y_i, y'_i \in Y$, $x_i, x'_i \in X$.

Докажем сначала, что (К) $\Rightarrow$ (Д). Для этого нужно доказать следующие два предложения:

1) $\forall q \in Q \forall \beta \in Y^* \forall k \in K \left|\bar{d}_q(\beta, k)\right| = |\beta|$;
2) $\forall q \in Q \forall \beta, \beta', \zeta \in Y^* \forall \tilde{\beta} \in Y^\tau \forall k \in K[(\bar{d}_q(\beta\tilde{\beta}\zeta, k) = \alpha\tilde{\alpha}\xi)\ \&\ (\bar{d}_q(\beta'\tilde{\beta}\zeta, k) = \alpha'\tilde{\alpha'}\xi') \Rightarrow (\xi = \xi')]$.

Первое предложение следует из определения функции $\bar{d}$. Для доказательства второго возьмем произвольные $q \in Q$, $\beta, \beta', \zeta \in Y^*$, $\tilde{\beta} \in Y^\tau$, $k \in K$. Пусть для некоторых $\alpha, \xi, \alpha', \xi'$ в X^*, $\tilde{\alpha}, \tilde{\alpha'}$ в X^τ, таких, что $|\xi| = |\xi'| = |\zeta|$, будет $\bar{d}_q(\beta\tilde{\beta}\zeta, k) = \alpha\tilde{\alpha}\xi$ и $\bar{d}_q(\beta'\tilde{\beta}\zeta, k) = \alpha'\tilde{\alpha'}\xi'$. Вычислим $q_\tau = \psi_k(q, \beta\tilde{\beta})$, $q'_\tau = \psi_k(q, \beta'\tilde{\beta})$, $\gamma = \gamma_\tau\gamma_{\tau+1}\dots\gamma_{l-1} = \bar{\varphi}_k(q_\tau, \zeta) = \bar{\varphi}_k(\psi_k(q, \beta\tilde{\beta}), \zeta)$ и $\gamma' = \gamma'_\tau\gamma'_{\tau+1}\dots\gamma'_{l-1} = \bar{\varphi}_k(q'_\tau, \zeta) = \bar{\varphi}_k(\psi_k(q, \beta'\tilde{\beta}), \zeta)$. В силу (К) имеет место $\bar{\varphi}_k(\psi_k(q, \beta\tilde{\beta}), \zeta) = \bar{\varphi}_k(\psi_k(q, \beta'\tilde{\beta}), \zeta)$, поэтому $\gamma = \gamma'$ и $x_i = d(y_i, \gamma_i) = d(y_i, \gamma'_i) = x'_i$ для $i = \tau, \tau+1, \dots, l-1$, т. е. $\xi = \xi'$. Таким образом, действительно (К) $\Rightarrow$ (Д).

Обратное следование (Д) $\Rightarrow$ (К) докажем от противного. Предположим, что не верно (К), то есть для некоторого ключа $k \in K$ проекция G_k ГКП G не является самосинхронизирующимся автоматом с задержкой τ и, следовательно,

$$\bar{\varphi}_k(\psi_k(q, \beta\tilde{\beta}), \zeta) \neq \bar{\varphi}_k(\psi_k(q, \beta'\tilde{\beta}), \zeta)$$

для некоторых $q \in Q, \beta, \beta', \zeta \in Y^*, \tilde{\beta} \in Y^\tau$. Пусть $\bar{\varphi}_k(\psi_k(q, \beta\tilde{\beta}), \zeta) = \gamma_\tau\gamma_{\tau+1}\dots\gamma_{l-1}$ и $\bar{\varphi}_k(\psi_k(q, y\beta' y\tilde{\beta}), \zeta) = \gamma'_\tau\gamma'_{\tau+1}\dots\gamma'_{l-1}$. Найдем такое t, что $\tau \leqslant t \leqslant l-1$ и $\gamma_\tau = \gamma'_\tau, \gamma_{\tau+1} = \gamma'_{\tau+1}, \dots, \gamma_{t-1} = \gamma'_{t-1}, \gamma_t \neq \gamma'_t$. Положим $\beta_0 = y_{-n}y_{-n+1}\dots y_{-1+t-\tau}$, $\tilde{\beta}_0 = y_{t-\tau}y_{1+t-\tau}\dots y_{\tau-1+t-\tau}$, $\zeta_0 = y_{\tau+t-\tau}y_{\tau+1+t-\tau}\dots y_{l-1}$ и $\beta'_0 = y_{-m}y_{-m+1}\dots y_{-1+t-\tau}$. Имеем: $\beta_0\tilde{\beta}_0\zeta_0 = \beta\tilde{\beta}\zeta$, $\beta'_0\tilde{\beta}_0\zeta_0 = \beta'\tilde{\beta}\zeta$, $\bar{\varphi}_k(\psi_k(q, \beta_0\tilde{\beta}_0), \zeta_0) = \gamma_t\gamma_{t+1}\dots\gamma_{l-1}$, $\bar{\varphi}_k(\psi_k(q, \beta'_0\tilde{\beta}_0), \zeta_0) = \gamma'_t\gamma'_{t+1}\dots\gamma'_{l-1}$ и $\gamma_t \neq \gamma'_t$.

Тем самым показано, что существуют такие $k \in K$, $q \in Q, \beta_0, \beta'_0 \in Y^*, \tilde{\beta}_0 \in Y^\tau$ и $y_t \in Y$, что $\gamma_t = \varphi_k(\psi_k(q, \beta_0\tilde{\beta}_0), y_t) \neq \varphi_k(\psi_k(q, \beta'_0\tilde{\beta}_0), y_t) = \gamma'_t$, или с учётом того, что G_k является автоматом Мура, $\gamma_t = \varphi_k(q_t) \neq \varphi_k(q'_t) = \gamma'_t$ для $q_t = \psi_k(q, \beta_0\tilde{\beta}_0)$ и $q'_t = \psi_k(q, \beta'_0\tilde{\beta}_0)$.

Пусть для любого $y \in Y$ и некоторых $\alpha, \alpha' \in X^*, \tilde{\alpha}, \tilde{\alpha'} \in X^\tau, x, x' \in X$

$$\bar{d}_q(\beta_0\tilde{\beta}_0 y, k) = \alpha\tilde{\alpha}x,\ \bar{d}_q(\beta'_0\tilde{\beta}_0 y, k) = \alpha'\tilde{\alpha'}x'.$$

Тогда по определению $\bar{d}$ будет $x = d(y, \varphi_k(q_t)) = d(y, \gamma_t)$ и $x' = d(y, \varphi_k(q'_t)) = d(y, \gamma'_t)$, а в силу (Д) — $x = x'$. Таким образом, $\forall y \in Y(d(y, \gamma_t) = d(y, \gamma'_t))$, откуда ввиду взаимной обратимости d и e следует $\forall x \in X(e(x, \gamma_t) = e(x, \gamma'_t))$, что противоречит отсутствию в Г эквивалентных символов. ■

5. Самосинхронизирующиеся автоматные шифрсистемы

Определение 10. 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

$$\sigma(y_{t-\tau}y_{t-\tau+1}\dots y_{t-1}, y_t) = y_{t-\tau+1}y_{t-\tau+2}\dots y_t.$$

Определение 11. 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 12. Назовем поточную шифрсистему $\Sigma_R = <X, K, Y, R, e, d>$ *регистровой*, если её ГКП R есть регистр сдвига с ключом. Длина регистра R называется размерностью шифрсистемы.

Для регистровых шифрсистем функцию шифрования $\bar{e}$ можно переписать в более простой форме:

$$\bar{e}(q_0, x_0x_1\dots x_{n-1}, k) = y_0y_1\dots y_{n-1}, \text{ где } \begin{cases} \gamma_t = \varphi_k(y_{t-\tau}y_{t-\tau+1}\dots y_{t-1}), \\ y_t = e(x_t, \gamma_t), \end{cases} \quad t = 0, 1, \dots, n-1.$$

Здесь $q_0 = y_{-\tau}y_{-\tau+1}\dots y_{-1}$.

Эти уравнения проиллюстрированы схемой рис. 3.

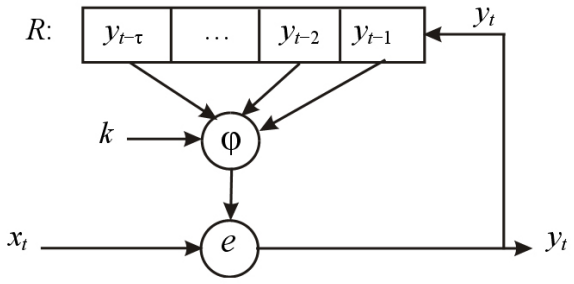

Рис. 3. Схема регистровой шифрсистемы

Регистровая шифрсистема размерностью τ является самосинхронизирующейся с задержкой τ по конструктивному определению. Как видно из следующей теоремы, в некотором смысле верно и обратное.

Теорема 5 [1]. Любая самосинхронизирующаяся с задержкой τ поточная шифрсистема с обратной связью $\Sigma_S = <X, Y, K, G, e, d>$, у которой все проекции G_k ГКП G суть сильно связные автоматы, неотличима от некоторой регистровой шифрсистемы $\Sigma_R = <X, Y, K, R, e, d>$ размерности τ.

Заметим, что в [5] под самосинхронизирующимися поточными шифрами понимаются именно регистровые шифрсистемы. Теорема 5 служит по существу теоретическим обоснованием такого понимания.

Определение 13. Назовём автоматную шифрсистему $\Sigma_A = <X, Y, K, E, D>$ *самосинхронизирующейся с задержкой* τ, если для её автомата расшифрования $D = <Y \times K, Q^*, X, \psi^*, \varphi^*>$ выполняется следующее условие:

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

Из определений 4, 7 и 13 непосредственно следует, что автоматная шифрсистема является самосинхронизирующейся с задержкой τ, если и только если этим свойством обладают все задаваемые ею последовательностные шифры.

Теорема 6. Любая самосинхронизирующаяся с задержкой τ автоматная шифрсистема $\Sigma_A = <X, K, Y, E, D>$, у которой все проекции E_k шифрующего автомата E суть сильно связные автоматы, неотличима от некоторой регистровой шифрсистемы $\Sigma_R = <X, K, Y, R, e, d>$ размерности τ.

Доказательство. Следуя доказательству теоремы 3, построим поточную шифрсистему $\Sigma_S = <X, Y, K, G, e, d>$, эквивалентную шифрсистеме $\Sigma_A = <X, Y, K, E, D>$. Поскольку шифрсистемы эквивалентны и шифрсистема Σ_A является самосинхронизирующейся с задержкой τ, то и шифрсистема Σ_S также является самосинхронизирующейся с задержкой τ.

Зафиксируем любое значение ключа $k \in K$ и рассмотрим в Σ_S проекцию G_k ГКП G на вход Y. По построению в доказательстве теоремы 3 функция переходов ГКП G определяется как

$$\psi'(q, (y, k)) = \psi(q, (\varphi_{qk}^{-1}(y), k)).$$

Соответственно этому функция переходов его проекции G_k определится как

$$\psi'_k(q, y) = \psi_k(q, \varphi_{qk}^{-1}(y)).$$

Поскольку по теореме 2 функция $\varphi_{qk}(x)$ инъективна, то обратная ей функция $\varphi_{qk}^{-1}(y)$ существует и сюръективна. В этом случае для любых $q_1, q_2 \in Q(= Q')$, $\alpha \in X^*$, $\beta \in Y^*$ если $\psi_k(q_1, \alpha) = q_2$ и $\bar{\varphi}_k(q_1, \alpha) = \beta$, то $\bar{\varphi}_k^{-1}(q_1, \beta) = \alpha$ и $\psi'_k(q_1, \beta) = \psi_k(q_1, \bar{\varphi}_{qk}^{-1}(\beta)) = \psi_k(q_1, \alpha) = q_2$, и из сильной связности автомата E_k следует сильная связность автомата G_k. Теперь по теореме 5 шифрсистема Σ_S, а вместе с ней и шифрсистема Σ_A, неотличима от некоторой регистровой шифрсистемы Σ_R размерности τ. ■

ЛИТЕРАТУРА

1. *Панкратов И. В.* К определению понятия самосинхронизирующегося поточного шифра // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 114–117.
2. *Панкратов И. В.* О поточных и автоматных шифрсистемах // Прикладная дискретная математика. Приложение. 2009. № 1. С. 21–24.
3. *Агибалов Г. П., Оранов А. М.* Лекции по теории конечных автоматов. Томск: Изд-во Том. ун-та, 1984. 185 с.
4. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.
5. *Menezes A., van Oorshot P., Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1996. 661 p.