МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

КОНЕЧНЫЕ АВТОМАТЫ В КРИПТОГРАФИИ

Г. П. Агибалов

Томский государственный университет, г. Томск, Россия

E-mail: agibalov@isc.tsu.ru

Сообщается о применениях конечных автоматов в качестве криптоалгоритмов и их компонент, известных из открытой литературы, в том числе в поточных и автоматных шифрсистемах, в симмметричных шифрах и криптосистемах с открытым ключом. Как автоматная шифрсистема описывется японская шифровальная машина времён Второй мировой войны Purple. Даются оценки числа попарно неэквивалентных ключей в шифре Закревского, построенного на основе сильносвязного конечного автомата с функцией выходов, биективной в каждом состоянии. Излагаются элементы теории симметричных поточных и автоматных шифрсистем, демонстрирующие функциональную эквивалентность их классов и неотличимость самосинхронизирующихся таких систем от регистровых.

Ключевые слова: *конечные автоматы, криптоавтоматы, генераторы ключевого потока, комбайнеры, клеточные автоматы, хеш-функции, симметричные шифры, последовательностные шифры, поточные шифрсистемы, автоматные шифрсистемы, регистровые шифрсистемы, самосинхронизирующиеся шифрсистемы, конечно-автоматные криптосистемы с открытым ключом, шифр Закревского, пурпурная машина.*

Введение

Конечные автоматы в криптографии распространены столь же широко, сколь и, скажем, целые числа, подстановки, булевы функции. Достаточно заметить, что все поточные шифры, ориентированные на аппаратную реализацию, допускают конструктивное описание как конечные автоматы канонической системой уравнений. Многочисленные примеры таких описаний поточных шифров конца прошлого века и их применения в криптоанализе можно найти, в частности, в [1, 2]. Вместе с тем в открытой научной литературе по современной криптографии конечные автоматы ещё не получили такого же широкого отражения, какое имеют другие дискретные структуры — те же целые числа или булевы функции. Особенно это касается теории автоматных криптосистем. Так, в отечественной литературе постсоветского периода можно указать лишь два источника монографического характера [3, 4], в которых хоть как-то упоминаются шифрующие автоматы.

В построении криптосистем конечные автоматы находят применение как в роли отдельных их компонент, начиная с регистров сдвига, так и в качестве полнофункциональных криптоалгоритмов — шифрования, цифровой подписи и т. п. В одних криптосистемах они выступают в чистом виде, в других — как криптографические автоматы (коротко: криптоавтоматы), конечно-автоматное поведение которых определяется ещё и в зависимости от ключа, выбираемого из некоторого конечного множества. Ключом

криптоавтомата могут быть и начальное состояние автомата, и некоторые элементы его таблиц переходов и выходов или сами эти таблицы — одна или обе сразу, и др.

В этой работе приводятся из открытой литературы последнего времени примеры употребления конечных автоматов и криптоавтоматов в роли генераторов ключевого потока и схем комбинирования (комбайнеров) в них, излагаются принципы построения клеточно-автоматных генераторов псевдослучайных последовательностей и ключевого потока и клеточно-автоматных хеш-функций, описываются конечно-автоматные симметричные шифры и криптосистемы с открытым ключом, демонстрируется функциональная эквивалентность поточных и автоматных шифрсистем и неотличимость самосинхронизирующихся таких систем от регистровых. Вопросы, относящиеся к криптоанализу, здесь не затрагиваются.

Предполагается знакомство читателя с основами теории автоматов и криптографии. В изложении, касающемся элементов теории автоматов, придерживаемся терминологии и обозначений из [5], а в употреблении криптографических понятий следуем за [6]. Кроме того, для любой функции f, для любого подмножества U её аргументов и для любого набора σ значений этих аргументов через f_σ обозначается функция (от остальных аргументов f), которая получается из f подстановкой под её знак вместо аргументов в U их значений в наборе σ.

1. Конечные автоматы

Конечный (полностью определённый) автомат M с множествами входных символов X, выходных символов Y и состояний Q и с функциями переходов $\psi : X \times Q \to Q$ и выходов $\varphi : X \times Q \to Y$ записывается как $M = <X, Q, Y, \psi, \varphi>$. В нём зависимость между входными символами, состояниями и выходными символами в дискретном времени t выражается системой канонических уравнений

$$\begin{cases} y(t) = \varphi(x(t), q(t)), \\ q(t+1) = \psi(x(t), q(t)), \end{cases} \qquad t = 1, 2, \ldots,$$

где $q(1)$ — начальное состояние автомата. Если здесь $\alpha = x(1)x(2)\ldots x(m)$, $\beta = y(1)y(2)\ldots y(m)$ и $\delta = q(2)q(3)\ldots q(m+1)$, то пишем: $\delta = \bar{\psi}(\alpha, q(1))$ — последовательность состояний, которую автомат M пробегает из состояния $q(1)$ под действием входного слова α; $\beta = \bar{\varphi}(\alpha, q(1))$ — выходное слово, которое он при этом вырабатывает; $q(m+1) = \psi(\alpha, q(1))$ — состояние, в которое он при этом переходит, и $y(m) = \varphi(\alpha, q(1))$ — выходной символ, который он выдаёт по завершении этого перехода.

В случае $X = A^n, Q = A^k, Y = A^m$ для натуральных n, k, m и алфавита A автомат M называется структурным, или автоматом в структурном алфавите A. В этом случае числа n, k и m называются размерностями соответственно входного символа, состояния и выходного символа, функции $\psi_i : A^n \times A^k \to A^k$ для $i = 1, 2, ..., k$ и $\varphi_j : A^n \times B^k \to A^m$ для $j = 1, 2, \ldots, m$, определяемые для любых $x \in A^n$ и $q \in A^k$ как $(\psi_1(x,q)\psi_2(x,q)\ldots\psi_k(x,q)) = \psi(x,q)$ и $(\varphi_1(x,q)\varphi_2(x,q)\ldots\varphi_m(x,q)) = \varphi(x,q)$, — структурными функциями соответственно переходов и выходов автомата M. Его каноническая система уравнений может быть записана в виде

$$\begin{cases} y_j(t) = \varphi_j(x_1(t)x_2(t)\ldots x_n(t), q_1(t)q_2(t)\ldots q_k(t)), \quad j = 1, 2, \ldots m, \\ q_i(t+1) = \psi_i(x_1(t)x_2(t)\ldots x_n(t), q_1(t)q_2(t)\ldots q_k(t)), \quad i = 1, 2, \ldots k, \end{cases} \qquad t = 1, 2, \ldots$$

Начальное состояние автомата в ней есть $q_1(1)q_2(1)\ldots q_k(1)$.

В случае, если $|X| = 1$ или функции в автомате M зависят фиктивно от входного символа, автомат M является автономным и записывается как $M = <Q, Y, \psi, \varphi>$, где $\psi : Q \to Q$ и $\varphi : Q \to Y$. Его канонические уравнения имеют вид

$$\begin{cases} y(t) = \varphi(q(t)), \\ q(t+1) = \psi(q(t)), \end{cases} \qquad t = 1, 2, \ldots,$$

или, в структурном алфавите,

$$\begin{cases} y_j(t) = \varphi_j(q_1(t)q_2(t)\ldots q_k(t)), \quad j = 1, 2, \ldots m, \\ q_i(t+1) = \psi_i(q_1(t)q_2(t)\ldots q_k(t)), \quad i = 1, 2, \ldots k, \end{cases} \qquad t = 1, 2, \ldots$$

Если в M функция $\varphi(x, q)$ зависит от x фиктивно, т. е. если M есть автомат Мура, то мы считаем, что фактически φ является отображением из Q в Q и пишем $\varphi(q)$ вместо $\varphi(x, q)$.

Наконец, если $|Q| = 1$, то автомат M называется комбинационным, или автоматом без памяти, и записывается как $M = <X, Y, \varphi>$, где $\varphi : X \to Y$.

В частичном автомате $M = <X, Q, Y, \psi, \varphi>$ функции ψ и φ являются частичными отображениями вида $\psi : D_\psi \subseteq X \times Q \to Q$ и $\varphi : D_\varphi \subseteq X \times Q \to Y$.

2. Криптоавтоматы

Криптоавтомат определяется формально как набор из шести объектов $C = <X, Q, Y, K, \psi, \varphi>$, в котором X, Q, Y, K — конечные множества, $K = Q_0 \times K_0$, $Q_0 \subseteq Q$, ψ, φ — функции, $\psi\colon K_0 \times X \times Q \to Q$ и $\varphi\colon K_0 \times X \times Q \to Y$. Множества X, Q, Y и функции ψ и φ играют по существу ту же роль, что и в конечном автомате M, и называются так же, как в M, — входным алфавитом, множеством состояний, выходным алфавитом и функциями переходов и выходов соответственно. Элементы в множестве $K = Q_0 \times K_0$ называются ключами. В произвольном ключе $k = (q_0, k_0) \in K$ компонента k_0 выступает в роли параметра, выделяющего в криптоавтомате C автомат $C_k = <X, Q, Y, \psi_k, \varphi_k>$, где функции $\psi_k\colon X \times Q \to Q$ и $\varphi_k\colon X \times Q \to Y$ для любых $x \in X$ и $q \in Q$ определяются как $\psi_k(x, q) = \psi(k_0, x, q)$ и $\varphi_k(x, q) = \varphi(k_0, x, q)$ и называются соответственно функциями переходов и выходов криптоавтомата C на ключе k. Автомат C_k называется *проекцией криптоавтомата C на ключе k*. Компонента q_0 в ключе k используется в качестве начального состояния автомата C_k.

В случае $|Q_0| > 1$ говорят, что криптоавтомат C *инициализируется по ключу*, или *имеет инициализирующий ключ*. В этом случае $q(1) \in Q_0$. Если, кроме того, $|K_0| = 1$ или каждая из функций $\psi(k_0, x, q)$, $\varphi(k_0, x, q)$ зависит от k_0 фиктивно, то криптоавтомат C записывается как $C = <X, Q, Y, Q_0, \psi, \varphi>$, подразумевая, что функции ψ и φ являются отображениями из $X \times Q$ в Q и Y соответственно. Говорят, что такой криптоавтомат C имеет *чисто инициализирующий ключ*, и множество ключей K в нём отождествляют с Q_0. Если же $|Q_0| = 1$, т. е. если криптоавтомат C не инициализируется по ключу, то предполагается, что $|K_0| > 1$ и хотя бы одна из его функций зависит существенно от k_0. Такой криптоавтомат C записывается как $C = <X, Q, Y, K_0, \psi, \varphi>$, и множество ключей K в нём отождествляется с K_0.

Нередко результаты теоретических исследований с участием понятия криптоавтомата не предполагают обязательности инициализируемости или неинициализируемости криптоавтомата по ключу, но обязательно предполагают, что $|K_0| > 1$ и хотя бы одна из его функций зависит существенно от $k_0 \in K_0$. За таким криптоавтоматом естественно сохранить обозначение произвольного криптоавтомата, но в отличие от

последнего называть его свободно инициализируемым — по ключу или нет и под K подразумевать только множество не инициализирующих ключей — K_0. Таким образом, *свободно инициализируемый криптоавтомат* — это $C = <X, Q, Y, K, \psi, \varphi>$, где $|K| > 1$, $\psi\colon K \times X \times Q \to Q$, $\varphi\colon K \times X \times Q \to Y$ и $\psi(k, x, q)$ или $\varphi(k, x, q)$ существенно зависят от k. В нём $q(1) \in Q$.

Автономный криптоавтомат определяется аналогично автономному автомату и записывается в общем случае как $C = <Q, Y, Q_0 \times K_0, \psi, \varphi>$. В нём, естественно, $\psi\colon K_0 \times Q \to Q$ и $\varphi\colon K_0 \times Q \to Y$, $\psi_k\colon Q \to Q$ и $\varphi_k\colon Q \to Y$ и $\psi_k(q) = \psi(k_0, q)$ и $\varphi_k(q) = \varphi(k_0, q)$ для любых $k = (q_0, k_0) \in K$ и $q \in Q$. Автономный криптоавтомат C, не инициализируемый по ключу, задаётся как $C = <Q, Y, K_0, \psi, \varphi>$, имеющий чисто инициализирующий ключ — как $C = <Q, Y, Q_0, \psi, \varphi>$ и свободно инициализируемый — как $C = <Q, Y, K, \psi, \varphi>$.

В случае, если все множества в криптоавтомате состоят из слов в некотором алфавите A, криптоавтомат называется *структурным*, или *криптоавтоматом в алфавите A*. Любой структурный криптоавтомат в некотором алфавите может быть задан подобно структурному автомату канонической системой уравнений со значениями переменных в этом алфавите.

Аналогично автомату Мура определяется *криптоавтомат Мура*, и как криптоавтомат он может быть инициализируемым или не инициализируемым по ключу, с чисто инициализирующим ключом, свободно инициализируемым или автономным и записываться соответствующим образом. *Комбинационный криптоавтомат*, или *криптоавтомат без памяти*, задаётся четвёркой $C = <X, Y, K, \varphi>$, где $\varphi\colon K \times X \to Y$.

3. Конечные автоматы и криптоавтоматы как компоненты криптосистем

3.1. Генераторы ключевого потока

Генераторы ключевого потока (ГКП) бывают синхронные, или без обратной связи, и асинхронные — с обратной связью. В первых ключевой поток вырабатывается в зависимости только от ключа шифра, а во вторых очередной символ ключевого потока зависит ещё и от нескольких предшествующих ему во времени символов шифртекста. Конечно-автоматный ГКП является некоторым криптоавтоматом, который в случае синхронного ГКП автономный, а в случае асинхронного ГКП — криптоавтомат Мура.

Примером синхронного конечно-автоматного ГКП может служить генератор MUGI [7], представляющий собой автономный криптоавтомат с чисто инициализирующим ключом $C = <Q, Y, Q_0, \psi, \varphi>$, в котором $Q = S \times B$, $S = A^3$, $B = A^{16}$, $A = \{0,1\}^{64}$, $Y = A$, $q = (s, b) \in S \times B$, $s = a_0 a_1 a_2 \in A^3$, $b = b_0 b_1 \dots b_{15} \in A^{16}$, элементы в $Q_0 \subseteq Q$ вычисляются с помощью некоторой процедуры инициализации по возможным значениям ключа шифра и вектора инициализации. Его канонические уравнения имеют вид

$$\begin{cases} y(t) = a_2(t), \\ a_0(t+1) = a_1(t), \\ a_1(t+1) = a_2(t) \oplus F(a_1(t), b_4(t)) \oplus C_1, \\ a_2(t+1) = a_0(t) \oplus F(a_1(t), b_{10}(t) <<< 17) \oplus C_2, \\ b_i(t+1) = b_{i-1}(t), i \neq 0, 4, 10, \\ b_0(t+1) = b_{15}(t) \oplus a_0(t), \\ b_4(t+1) = b_3(t) \oplus b_7(t), \\ b_{10}(t+1) = b_9(t) \oplus (b_{13}(t) <<< 32), \end{cases} \qquad t \geqslant 1,$$

где $\oplus$ есть побитное сложение по mod 2, $c <<< r$ — результат циклического сдвига числа c на r разрядов влево, $C_1 =$ BB67AE8584CAA73B, $C_2 =$ 3C6EF372FE94F82B и $F(u,v)$ для u,v в A определяется как $F(u,v) = \pi(\mu(\sigma(u \oplus v)))$, где σ — простая побайтная замена, μ — линейное преобразование (умножением на матрицу) и $\pi(B_0B_1\dots B_7) = B_4B_5B_2B_3B_0B_1B_6B_7$ для последовательности байт $B_0, B_1, \dots, B_7$.

В качестве примера асинхронного конечно-автоматного ГКП рассмотрим генератор KNOT [8]. Он представляет собой не инициализируемый ключом криптоавтомат Мура $C = <X, Q, Y, K_0, \psi, \varphi>$ с $X = Y = \{0,1\}$, $Q = \{0,1\}^{128}$, $K_0 = \{0,1\}^{96}$. В нём каждое состояние $q \in Q$ является булевым вектором с компонентами q_{ij} для всех $ij \in I$, где $I = \{ij : i = 1,2,\dots,88, j = 0; i = 89,90,91,92, j = 0,1; i = 93,94, j = 0,1,2,3; i = 95, j = 0,1,\dots,7; i = 96, j = 0,1,\dots,15\}$. Его каноническая система уравнений имеет следующий вид:

$$\begin{cases} y(t) = R_8(\cdots R_2(R_1(q(t)))), \\ q_{ij}(t+1) = f_{ij}(a_{ij}(t), b_{ij}(t), c_{ij}(t), d_{ij}(t)), \quad ij \in I, \end{cases}$$

где $R_i : \{0,1\}^{n_{i-1}} \to \{0,1\}^{n_i}$ для $i = 1,2,\dots,8$; $n_0 = 128$, $n_1 = n_2 = 64$, $n_3 = n_4 = 32$, $n_5 = n_6 = 16$, $n_7 = 8$, $n_8 = 1$; $R_i(x_0x_1\dots x_{n_{i-1}-1}) = g(x_{6i}x_{6i+3}x_{6i+1}x_{6i+2})$ для $i = 1,3,5,7$, $R_i(x_0x_1\dots x_{n_{i-1}-1}) = g(x_{5i}x_{6i+3}x_{5i+1}x_{5i+2})$ для $i = 2,4,6$ со сложением в индексах по модулю n_i и $R_8(x_0x_1\dots x_7) = x_0 \oplus x_1(x_2 \oplus 1) \oplus 1$;
$f_{ij} \in \{g, h\}$, $ij \in I$;
$g(a,b,c,d) = a \oplus b \oplus c(d \oplus 1) \oplus 1$, $h(a,b,c,d) = a(b \oplus 1) \oplus c(d \oplus 1)$;
$a_{ij}(t), b_{ij}(t), c_{ij}(t), d_{ij}(t) \in \{q_{ij}(t) : ij \in I\} \cup \{k_0, k_1, \dots, k_{95}\} \cup \{0, c_t\}$, $t \geqslant 1$;
$k_0k_1\dots k_{95} \in K_0$ и c_t есть t-й символ шифртекста; $t = 1,2,\dots$

3.2. Комбайнеры в генераторах ключевого потока

Комбайнер является обязательной составляющей всякого генератора ключевого потока комбинирующего типа. С его помощью в таком генераторе несколько последовательностей символов «комбинируются» в некоторые другие (одну или более) посредством некоторого преобразования (функции). В этом смысле такая разновидность генератора ключевого потока, как фильтрующий генератор, является по существу комбайнером: в нём в одну комбинируются последовательности символов, снимаемых с разрядов некоторого регистра. Далее фильтрующие генераторы рассматриваются не отдельно от комбинирующих, но как их частный случай. В конечно-автоматном комбайнере символы всех последовательностей, участвующих в комбинировании, принадлежат обычно некоторому одному алфавиту A, а сам комбайнер представляет собой автомат вида $M = <A^n, Q, A^m, \psi, \varphi>$, где $n \geqslant 2$, $m \geqslant 1$.

Примером простейшего такого комбайнера служит последовательностный сумматор. В нём $A = \{0,1\}$, $Q = \{0,1,\dots,n-1\}$, $m = 1$, $\psi(x_1x_2\dots x_n, q) = \lfloor \sigma/2 \rfloor$, $\varphi(x_1x_2\dots x_n, q) = \sigma \bmod 2$, где $\sigma = x_1 + x_2 + \dots + x_n + q$.

В комбайнере M генератора Bluetooth [9] $A = \{0,1\}$, $n = 4$, $Q = \{0,1\}^4$, входной символ и состояние являются булевыми векторами $x = x_1x_2x_3x_4$ и $q = q_1q_2q_3q_4$ соответственно, $\varphi(x,q) = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus q_3$ и $\psi(x,q) = (q_3, q_4, s_1 \oplus q_1 \oplus q_2 \oplus q_3, s_2 \oplus q_1 \oplus q_4)$, где s_1s_2 есть двоичное представление числа $\lfloor (x_1 + x_2 + x_3 + x_4 + q_3 + 2q_4)/2 \rfloor$.

Комбайнер в ГКП VEST [10] представляет собой последовательное соединение двух автоматов Мура $M_1 \times M_2$ — линейного автомата $M_1 = <\{0,1\}^{16}, \{0,1\}^{10}, \{0,1\}^{10}, \delta, \lambda>$, в котором для входного символа $x = x_0x_1\dots x_{15}$ и состояния $q = d_0d_1\dots d_9$ выполня-

ются равенства

$$\lambda(q) = q, \quad \delta(x,q) = \delta_0(x,q)\delta_1(x,q)\dots\delta_9(x,q),$$
$$\delta_0(x,q) = d_1 \oplus x_1 \oplus x_4 \oplus x_5 \oplus x_{11} \oplus x_{13},$$
$$\delta_1(x,q) = d_2 \oplus x_0 \oplus x_2 \oplus x_6 \oplus x_8 \oplus x_{14},$$
$$\delta_2(x,q) = d_3 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_{10} \oplus x_{15},$$
$$\delta_3(x,q) = d_4 \oplus x_0 \oplus x_3 \oplus x_5 \oplus x_9 \oplus x_{12},$$
$$\delta_4(x,q) = d_5 \oplus x_1 \oplus x_4 \oplus x_6 \oplus x_{12} \oplus x_{15} \oplus 1,$$
$$\delta_5(x,q) = d_6 \oplus x_0 \oplus x_7 \oplus x_9 \oplus x_{13} \oplus x_{14},$$
$$\delta_6(x,q) = d_7 \oplus x_1 \oplus x_8 \oplus x_{11} \oplus x_{14} \oplus x_{15},$$
$$\delta_7(x,q) = d_8 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_{10} \oplus x_{12} \oplus 1,$$
$$\delta_8(x,q) = d_0 \oplus x_0 \oplus x_3 \oplus x_7 \oplus x_8 \oplus x_9 \oplus 1,$$
$$\delta_9(x,q) = d_9 \oplus x_8 \oplus x_{10} \oplus x_{12} \oplus x_{13} \oplus x_{15} \oplus 1,$$

и нелинейного автомата $M_2 = <\{0,1\}^{10}, \{0,1\}^w, \{0,1\}^m, \psi, \varphi>$, в котором для входного символа $x = d_0d_1\dots d_9$ и состояния $q = q_0q_1\dots q_{w-1}$ имеют место равенства

$$\varphi(q) = \varphi_0(q)\varphi_1(q)\dots\varphi_{m-1}(q),$$
$$\psi(q) = \psi_0(x,q)\psi_1(x,q)\dots\psi_{w-1}(x,q),$$
$$\varphi_j(q) = q_{j_0} \oplus q_{j_1} \oplus \dots \oplus q_{j_5}, \quad j = 0,1,\dots,m-1,$$
$$\psi_{p_i}(x,q) = f_i(q_0,q_1,q_2,q_3,q_4) \oplus d_i, \quad 0 \leqslant i < 5,$$
$$\psi_{p_i}(x,q) = f_i(q_{i_0},q_{i_1},q_{i_2},q_{i_3},q_{i_4}) \oplus q_i \oplus d_i, \quad 5 \leqslant i < 10,$$
$$\psi_{p_i}(x,q) = f_i(q_{i_0},q_{i_1},q_{i_2},q_{i_3},q_{i_4}) \oplus q_i, \quad 10 \leqslant i < w,$$

для некоторых различных $j_0, j_1, \dots, j_5$ в $\{0,1,\dots,w-1\}$, различных $i_0, i_1, \dots, i_4$ в $\{0,1,\dots,w-1\}$, различных $p_0, p_1, \dots, p_{w-1}$ в $\{0,1,\dots,w-1\}$, $f_i : \{0,1\}^5 \to \{0,1\}$ и $(w,m) \in \{(83,4),(211,8),(331,16),(587,32)\}$.

4. Клеточные автоматы как компоненты криптосистем

Говорят, что задан клеточный автомат CA (сокращённо от Cellular Automaton), если заданы:

1) натуральные l и r, такие, что $l \geqslant r \geqslant 2$, числа $1,2,\dots,l$ суть номера ячеек в CA и r — мощность окрестности любой его ячейки;

2) булева функция $\eta\colon \{0,1\}^r \times \{0,1\} \to \{0,1\}$, называемая функцией переходов ячейки в CA;

3) для каждого $i \in \{1,2,\dots,l\}$ множество $\theta(i) = \{i_1, i_2, \dots, i_r\}$ номеров $i_1 < i_2 < \dots < i_r$ всех ячеек в окрестности ячейки с номером i.

Состояниями ячейки в CA являются элементы множества $\{0,1\}$, а состояниями самого CA — элементы множества $Q = \{0,1\}^l$. Функцией переходов CA является функция $\psi\colon Q \to Q$, определяемая для любого состояния $q_1q_2\dots q_l$ как $\psi(q_1q_2\dots q_l) = s_1s_2\dots s_l \in Q$, где $s_i = \eta(q_{i_1}q_{i_2\dots}q_{i_r}, q_i)$ и $\{i_1,i_2,\dots,i_r\} = \theta(i)$, $i = 1,2,\dots,l$. Функции $\psi^t\colon Q \to Q$, определяемые для всех натуральных $t \geqslant 1$ индукцией по t как $\psi^1 = \psi$ и $\psi^{t+1}(q) = \psi(\psi^t(q))$ для любого $q \in Q$, называются операциями CA.

Клеточно-автоматный генератор псевдослучайной последовательности (ПСП) строится на базе CA как некоторый автономный автомат $M = <Q, Y, \psi, \varphi>$, в котором Q и ψ суть соответственно множество состояний и функция переходов CA, $Y = \{0,1\}^m$, $\varphi\colon Q \to Y$, $\varphi(q_1\dots q_l) = q_{j_1}\dots q_{j_m}$ для некоторых $m \geqslant 1$ и $1 \leqslant j_1 < \dots < j_m \leqslant l$.

Синхронный клеточно-автоматный ГКП [11] в общем случае является некоторым автономным криптоавтоматом $C = <Q, Y, K, \psi, \varphi>$, где Q и ψ_k для каждого $k \in K = Q_0 \times K_0$ суть соответственно множество состояний и функция переходов некоторого CA. В частном случае криптоавтомат C здесь может быть не инициализируемым по

ключу или иметь чисто инициализирующий ключ, а алфавит Y и функции φ_k, $k \in K$, в нём — такими же, как Y и φ в генераторе ПСП.

Бесключевые хеш-функции вида $f\colon \{0,1\}^* \to \{0,1\}^m$ строят обычно по следующей общей схеме. Подлежащий хешированию текст $\alpha \in \{0,1\}^*$ предварительно расширяют до длины, кратной некоторому числу n, и разбивают на блоки длины n, представляя его, таким образом, конкатенацией $P_1P_2\ldots P_N$ блоков разбиения. Затем, выбрав некоторое $H_0 \in \{0,1\}^m$ и применяя некоторую функцию $h\colon \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^m$, называемую функцией сжатия, выполняют итеративно вычисления

$$H_i = h(P_i, H_{i-1}), i = 1, 2, \ldots, N-1,$$

после чего полагают $f(\alpha) = g(H_N)$ для некоторой функции $g\colon \{0,1\}^m \to \{0,1\}^m$, называемой функцией выхода.

Разные хеш-функции получаются по этой схеме с разными функциями сжатия и выхода. В схемах для построения клеточно-автоматных хеш-функций [12] процедуры, определяющие функции сжатия и выхода, наряду с другими (логическими и арифметическими) операциями используют операции CA.

5. Конечно-автоматные симметричные шифры

5.1. Пурпурная машина

Японская шифровальная машина времён Второй мировой войны Angooki Taipu, известная в криптографии под названием Purple (пурпурная), является, по-видимому, первым шифром, построенным на конечных автоматах. И хотя в ту пору понятия конечного автомата ещё не существовало, и первое представление о нём как о дискретном преобразователе с конечным числом возможных состояний, применимом в качестве схем кодирования и декодирования информации, появилось только в 1948 г. в знаменитой статье Клода Шеннона [13], а современные источники (см., например, [14]) подают эту машину по-прежнему на архаичном языке, — несмотря на всё это, адекватное и значительно более простое описание машины Purple возможно именно в конечно-автоматных терминах, более близких современному специалисту.

Схема шифрования машины Purple изображена на рис. 1.

В ней, кроме входной и выходной коммутационных панелей для простой замены символов открытого текста и символов шифртекста соответственно, центральное место занимают блоки L, M, R, S и stepping, являющиеся конечными криптоавтоматами, причём $L = M = R$. Первые четыре криптоавтомата имеют чисто инициализирующие ключи и выступают в роли автоматов-преобразователей, а последний (stepping) является комбинационным криптоавтоматом и служит в роли управляющего автомата, определяющего порядок смены состояний в первых трёх. В автоматах L, M, R, S состояниями являются целые $0, 1, \ldots, 24$, и в каждом из них состояние q под действием входного символа может либо сохраниться, либо измениться к состоянию $q+1 \mod 25$. В зависимости от ключа шифра криптоавтоматы L, M, R подразделяются на «быстрый» — f, «средний» — m и «медленный» — s. Криптоавтомат S изменяет своё состояние под действием каждого входного символа, а среди криптоавтоматов L, M, R это делает только один, выбираемый управляющим криптоавтоматом stepping в зависимости от состояний S и «среднего» так, что «быстрый» изменяет своё состояние всякий раз за исключением следующих двух случаев:

1) если S находится в состоянии 24, то состояние меняет «средний»;

2) если S в состоянии 23, а «средний» — в 24, то состояние меняет «медленный».

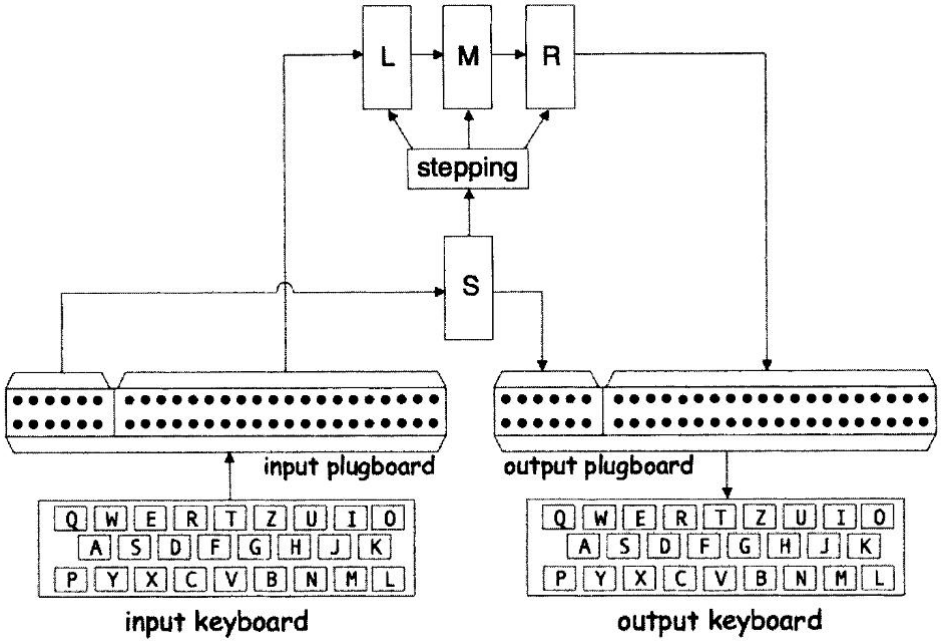

Рис. 1. Шифрование в Purple

Соответственно этому все каналы связи между компонентами машины подразделяются на информационные и управляющие. По первым передаются символы латинского алфавита, являющегося алфавитом шифра, а по вторым — символы состояний (от L, M, R, S к stepping) и логические 0, 1 (от stepping к L, M, R). Последние два символа взяты нами произвольно для обозначения управляющих команд «сохранить состояние», «изменить состояние» соответственно. По информационным каналам, связанным с автоматом S, передаются гласные латинские буквы, а по информационным каналам, связанным с L, M, R, — согласные латинские буквы.

Функция информационного выхода каждого автомата-преобразователя при любой фиксации его состояния и символа управляющего входа, если он есть, является некоторой биекцией на соответствующем информационном алфавите (составленном из букв на информационных каналах этого автомата).

Перейдём теперь к формальному описанию всех перечисленных криптоавтоматов в машине Purple.

Каждый из криптоавтоматов $C \in \{L, M, R, S\}$ имеет вид $C = <X_C, Q, Q_0, Y_C, \psi_C, \varphi_C>$, где $Q_0 = Q = Z_{25}$; $X_S = A_6 = \{\text{A, E, I, O, U, Y}\}$ — множество латинских гласных, $Y_S = A_6 \times Q$; $X_C = A_{20} \times \{0, 1\}$, $Y_C = A_{20} \times Q$, где $A_{20} = (\{\text{A, B,}\ldots, \text{Z}\} \setminus A_6)$ — множество латинских согласных, — для $C \in \{L, M, R\}$;

$$\psi_C(x, q) = \begin{cases} q, \text{ если } C \in \{L, M, R\}, x = a0 \text{ и } a \in A_{20}, \\ q + 1 \bmod 25 \text{ в противном случае, т. е. если } C = S, \text{либо } x = a1 \text{ и } a \in A_{20}; \end{cases}$$

$$\varphi_C(x, q) = \begin{cases} (\delta(a, q), q), \text{ если } C \in \{L, M, R\}, x = au \in X_C \text{ и } q \in Q, \\ (\varepsilon(x, q), q), \text{ если } C = S, x \in X_S \text{ и } q \in Q, \end{cases}$$

для некоторых функций $\delta\colon A_{20} \times Q \to A_{20}$ и $\varepsilon\colon A_6 \times Q \to A_6$, таких, что для всех $q \in Q$ функции $\delta_q\colon A_{20} \to A_{20}$ и $\varepsilon_q\colon A_6 \to A_6$ суть различные биекции.

В комбинационном криптоавтомате stepping $<X, Y, K, \varphi>$: $X = Q^4$, $Y = \{001, 010, 100\}$, $K = \{fms, fsm, mfs, msf, sfm, smf\}$,

$$\varphi(k, q_L q_M q_R q_S) = \begin{cases} 001, & \text{если } k = fms, q_M = 24, q_S = 23; k = fsm, q_S = 24; \\ & \quad k = mfs, q_L = 24, q_S = 23; \\ & \quad k = msf, q_S \neq 24 \text{ и } (q_L, q_S) \neq (24, 23); \\ & \quad k = sfm, q_S = 24; k = smf, q_s \neq 24 \text{ и } (q_M, q_S) \neq (24, 23); \\ 010, & \text{если } k = fms, q_S = 24; k = fsm, q_R = 24, q_S = 23; \\ & \quad k = mfs, q_S \neq 24 \text{ и } (q_L, q_S) \neq (24, 23); \\ & \quad k = msf, q_L = 24, q_S = 23; \\ & \quad k = sfm, q_s \neq 24 \text{ и } (q_R, q_S) \neq (24, 23); k = smf, q_S = 24; \\ 100, & \text{если } k = fms, q_S \neq 24 \text{ и } (q_M, q_S) \neq (24, 23); \\ & \quad k = fsm, q_S \neq 24 \text{ и } (q_R, q_S) \neq (24, 23); \\ & \quad k = mfs, q_S = 24; k = msf, q_S = 24; \\ & \quad k = sfm, q_R = 24, q_s = 23; k = smf, q_M = 24, q_S = 23. \end{cases}$$

Расшифрование в машине Purple выполняется по схеме, которая получается из схемы на рис. 1 поворотом стрелок на информационных каналах в противоположную сторону и заменой автоматов L, M, R, S обратными (на информационных каналах) автоматами L^{-1}, M^{-1}, R^{-1}, S^{-1} соответственно, получаемыми из первых заменой функций δ и ε функциями δ' и ε' соответственно, где для $\sigma \in \{\delta, \varepsilon\}$ функция σ' определяется как $\sigma'(x, q) = y$, если $\sigma(y, q) = x$.

5.2. Шифр Закревского

Как другой пример симметричного конечно-автоматного шифра рассмотрим шифр, предложенный А. Д. Закревским в рукописи от 1959 г., опубликованной впервые в [15]. В наших терминах шифр Закревского является инициализируемым по ключу криптоавтоматом $C = <X, Q, Y, K, \psi, \varphi>$, в котором множество ключей $K = Q \times K_0$ таково, что $\Upsilon = \{C_k = <X, Q, Y, \psi_k, \varphi_k> : k \in K\}$ есть множество всех сильносвязных автоматов с фиксированными алфавитами X, Q, Y и биективными функциями $\varphi_{kq} \colon X \to Y$, определяемыми при любых $k \in K$ и $q \in Q$ как $\varphi_{kq}(x) = \varphi(k, x, q)$ для всех $x \in X$. На ключе $k = (q_0, k_0) \in K$ сообщение $\alpha \in X^*$ зашифровывается автоматом C_k из «ключевого» (определяемого ключом k) начального состояния $q_0 \in Q$ в криптограмму $\beta = \bar{\varphi}_k(\alpha, q_0) \in Y^*$, которая расшифровывается в сообщение $\alpha = \bar{\varphi}'_k(\beta, q_0)$ автоматом $D_k = <Y, Q, X, \psi'_k, \varphi'_k>$, где функции ψ'_k и φ'_k определяются по правилу: если $\psi_k(x, q) = s$ и $\varphi_k(x, q) = y$, то $\psi'_k(y, q) = s$ и $\varphi'_k(y, q) = x$ для всех $x \in X$, $y \in Y$, $q \in Q$.

Пусть в C здесь $|X| = |Y| = m$ и $|Q| = n$. Тогда непосредственно подсчитывается, что $|\Upsilon| > n^{(m-1)n} n^{m!}$.

Два ключа k и k' в K называются *эквивалентными*, если автоматы C_k, $C_{k'}$ в Υ осуществляют одно и то же отображение из X^* в Y^* из своих «ключевых» начальных соостояний $q_0, q'_0 \in Q$ соответственно, т. е. если $\bar{\varphi}_{k,q_0} = \bar{\varphi}_{k',q'_0}$. Обозначим $\varkappa$ количество всех классов эквивалентности ключей в K, или, что то же самое, число всех попарно неэквивалентных ключей рассматриваемого шифра.

Теорема 1. $\varkappa \leqslant \dfrac{(mn)^{mn}}{(n-1)!}$.

Доказательство. Автомат с m входными символами, n состояниями и r выходными символами называется (m, n, r)-автоматом. Пусть далее $C_{m,n,r}$ есть класс всех сильно-связных приведенных и попарно не эквивалентных (m, l, r)-автоматов с общим

входным алфавитом, с общим выходным алфавитом и с l состояниями $1, 2, \ldots, l$ для всевозможных $l \leqslant n$. Имеем: $\varkappa \leqslant n \cdot |C_{m,n,m}|$. Оценим число $|C_{m,n,r}|$. Для этого установим некоторые вспомогательные предложения.

Для автомата $M = <X, Q, Y, \psi, \varphi>$ и биекции $h\colon Q \to Q$ определим автомат $hM = <X, Q, Y, \psi', \varphi'>$, где $\forall x \in X \forall q \in Q(\psi'(x, hq) = h\psi(x, q) \wedge \varphi'(x, hq) = \varphi(x, q))$. Назовём его *изоморфным по состояниям* автомату M (при *изоморфизме* h). По определению, hM получается из M перестановкой состояний в соответствии с h, а именно: на месте q в M стоит hq в hM. Индукцией по $|\alpha|$ непосредственно проверяется, что $\forall \alpha \in X^* \forall q \in Q(\psi'(\alpha, hq) = h\psi(\alpha, q) \wedge \varphi'(\alpha, hq) = \varphi(\alpha, q))$, откуда следует, что состояние q в M и состояние hq в hM эквивалентны и, следовательно, $M \sim hM$. Из последнего также следует, что изоморфность по состояниям автоматов влечет их эквивалентность и что приведенность M равносильна приведенности hM. Кроме того, для приведённого M и нетождественной h верно $M \neq hM$, так как иначе $\forall \alpha \in X^* \forall q \in Q(\varphi(\alpha, hq) = \varphi'(\alpha, hq) = \varphi(\alpha, q))$, т. е. для каждого $q \in Q$ состояния q и hq неотличимы в M, что при $hq \neq q$ противоречит приведённости M. Это утверждение, в свою очередь, влечёт следующее: $h_1 M \neq h_2 M$, если $h_1 \neq h_2$, так как иначе $h_2^{-1} h_1 M = M$. Обозначим $I(M)$ множество автоматов, изоморфных по состояниям автомату M при всевозможных изоморфизмах $h\colon Q \to Q$. Если $|Q| = n$, то количество последних равно $n!$ и в силу последнего утверждения для приведённого автомата M с n состояниями $|I(M)| = n!$. Наконец для автоматов M_1 и M_2, не изоморфных по состояниям, $I(M_1) \cap I(M_2) = \varnothing$, так как иначе для некоторого автомата $M \in I(M_1) \cap I(M_2)$ и некоторых изоморфизмов h_1 и h_2 будем иметь $h_1 M_1 = M = h_2 M_2$, откуда $h_2^{-1} h_1 M_1 = M_2$ и M_2 изоморфен M_1.

Обозначим $R_{m,n,r}$ множество всех сильносвязных приведённых и попарно не изоморфных по состояниям (m, l, r)-автоматов с общим входным алфавитом, с общим выходным алфавитом и с l состояниями $1, 2, \ldots, l$ для всевозможных $l \leqslant n$. Имеем: $C_{m,n,r} \subseteq R_{m,n,r}$ и $|C_{m,n,r}| \leqslant |R_{m,n,r}|$. Оценим последнее число. Для этого воспользуемся методом Э. Ф. Мура из [16]. Для любого (m, l, r)-автомата M с $l \leqslant n$ определим (m, n, r)-автомат M' по следующим правилам: 1) если $l = n$, то $M' = M$; 2) если $l < n$, то M' получается из M присоединением к M новых $n - l$ состояний $l + 1, \ldots, n$ и новых переходов: для каждого входного символа с выдачей некоторого выходного — из состояния i в состояние $i + 1$ для $i = l + 1, \ldots, n - 1$ и из состояния n в некоторое состояние в M. По определению, если M приведён, то приведён и M'. В этом случае $|I(M')| = n!$. Каждому автомату $M \in R_{m,n,r}$ поставим в соответствие множество автоматов $I(M')$. Ввиду приведенности и попарной неизоморфности автоматов в $R_{m,n,r}$, разным автоматам в $R_{m,n,r}$ будут тем самым сопоставлены непересекающиеся множества (m, n, r)-автоматов с $n!$ автоматами в каждом. Следовательно, $n! |R_{m,n,r}| \leqslant (nr)^{mn}$ — число всех (m, n, r)-автоматов с общими соответственно входными, выходными и внутренними алфавитами. Отсюда $|R_{m,n,r}| \leqslant \dfrac{(nr)^{mn}}{n!}$. Таким образом, $\varkappa \leqslant n \cdot |C_{m,n,m}| \leqslant n \cdot |R_{m,n,m}| \leqslant \dfrac{(mn)^{mn}}{(n-1)!}$. ■

Теорема 2. $m^n \leqslant \varkappa$.

Доказательство. Зафиксируем целые $m, n \geqslant 2$, алфавиты X, Y одной мощности — m, $Q = \{1, 2, \ldots, n\}$ и слово $\alpha = a_1 a_2 \ldots a_n \in X^n$. Для любого $\beta = b_1 b_2 \ldots b_n \in Y^n$ определим такой автомат $M_\beta = <X, Q, Y, \psi, \varphi>$ с биективными $\varphi_q\colon X \to Y$ для всех $q \in Q$, в котором $\psi(a_i, i) = i + 1$ для $i = 1, 2, \ldots n - 1$, $\psi(x, q) = 1$ в остальных слу-

чаях и $\varphi(a_i, i) = b_i$ для $i = 1, 2, \ldots n$. Пусть $\Upsilon_\alpha = \{M_\beta : \beta \in Y^n\}$. По определению $\bar{\psi}(\alpha, 1) = 23 \ldots n1$ и автомат M_β сильно связен. Следовательно, $\Upsilon_\alpha \subseteq \Upsilon$. Кроме того, если $\beta \neq \beta'$, то $M_\beta \neq M_{\beta'}$, состояние 1 в M_β отличимо (входным словом α) от состояния 1 в $M_{\beta'}$, и значит, автоматы M_β и $M_{\beta'}$ в состоянии 1 осуществляют разные отображения из X^* в Y^*. Осталось только заметить, что $|\Upsilon_\alpha| = |\{\beta\colon \beta \in Y^n\}| = m^n$. ■

6. Поточные и автоматные шифрсистемы

6.1. Введение

Содержание этого раздела относится исключительно к теории последовательностного шифрования и имеет целью выяснение соотношения между симметричными поточными и конечно-автоматными шифрсистемами, в том числе самосинхронизирующимися с конечной задержкой. Излагаются результаты, полученные в 2006–2008 гг. студентом И. В. Панкратовым в курсовой и дипломной работах, которые выполнены им под руководством автора и опубликованы в [17 – 19].

Даются формальные определения симметричных поточных и автоматных шифрсистем и задаваемых ими последовательностных шифров. Показываются неотличимость поточных шифрсистем с неотличимыми генераторами ключевого потока и 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. Даются конструктивное и дескриптивное определения самосинхронизирующейся с задержкой поточной шифрсистемы и показывается их равносильность. Первое определение предполагает самосинхронизируемость с задержкой криптоавтомата ключевого потока системы при каждом значении её ключа, а второе — самосинхронизируемость с задержкой каждого последовательностного шифра, задаваемого этой шифрсистемой. Определяются регистр сдвига как автомат с конечной входной памятью, регистр сдвига с ключом и регистровая шифрсистема как частный случай самосинхронизирующейся поточной шифрсистемы. Показываются сильная неотличимость сильносвязного самосинхронизирующегося автомата Мура от регистра сдвига и неотличимость от регистровой шифрсистемы любой поточной шифрсистемы с сильносвязным генератором ключевого потока при каждом значении ключа. Определяется самосинхронизирующаяся с задержкой автоматная шифрсистема и показывается, что регистровыми шифрсистемами исчерпываются с точностью до неотличимости и все автоматные самосинхронизирующиеся шифрсистемы с сильносвязными на каждом ключе автоматами шифрования.

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.

6.2. Поточные шифрсистемы

Определение 2. Назовём *поточной шифрсистемой* набор из шести объектов $\Sigma_S = <X, Y, K, G, e, d>$, где $G = <Y, Q, Z, K, \psi, \varphi>$ — свободно инициализируемый криптоавтомат, называемый *генератором ключевого потока (ГКП)*, такой, что любая его проекция G_k, $k \in K$, есть автомат Мура, $e\colon X \times Z \to Y$ и $d\colon Y \times Z \to X$ суть правила соответственно шифрования и расшифрования одного символа (открытого текста и шифртекста) с помощью одного символа ключевого потока, связанные отношением обратимости

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

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* (открытого текста) и *расшифрования* (шифртекста), которые по ключу $k \in K$ и начальному состоянию $q_0 \in Q$ определяются по следующим формулам:

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

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

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

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

Эти уравнения проиллюстрированы схемами на рис. 2 и 3, где D обозначает элемент задержки на единицу дискретного времени. В них последовательности $q_0 q_1 \dots$ и $z_0 z_1 \dots$ 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 $y_0 y_1 \dots$

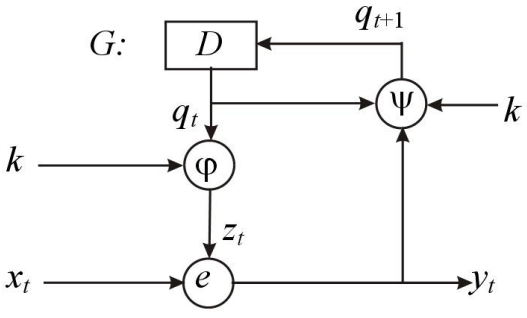

Рис. 2. Схема алгоритма шифрования в поточной шифрсистеме

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 $\bar{e}_q(\alpha, k) = \bar{e}(q, \alpha, k)$, $\bar{d}_q(\beta, k) = \bar{d}(q, \beta, k)$ 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.

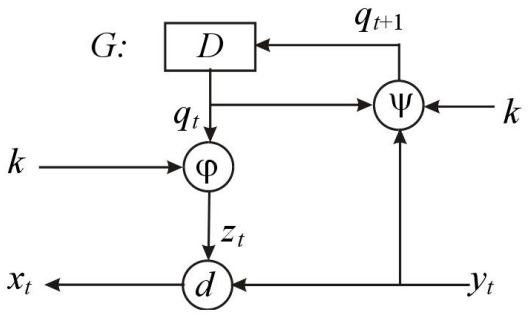

Рис. 3. Схема алгоритма расшифрования в поточной шифрсистеме

Определение 3. Поточную шифрсистему $\Sigma_S = <X, Y, K, G, e, d>$ будем называть *неотличимой* от поточной шифрсистемы $\Sigma'_S = <X, Y, K, G', e', d'>$, где $G = <Y, Q, Z, K, \psi, \varphi>$ и $G' = <Y, Q', Z', K, \psi', \varphi'>$, если выполняется следующее условие:

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

Заметим, что неотличимость двух поточных шифрсистем друг от друга в этом смысле вовсе не означает равенства семейств задаваемых ими последовательностных шифров. Это было бы так, если бы вместо неотличимости рассматриваемых шифрсистем речь шла об их сильной неотличимости, где Σ_S *сильно неотличима* от Σ'_S, если выполнено условие

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

Последнее отличается от предыдущего только порядком применения кванторов и означает как раз включение $S(\Sigma_S) \subseteq S(\Sigma'_S)$. Поскольку для любого предиката $P(a, b)$ из $\exists a \forall b P(a, b)$ следует $\forall b \exists a P(a, b)$, но не наоборот, то сильная неотличимость ($\cong$) шифрсистем влечёт их неотличимость ($\approx$), а обратного может не быть. Таким образом, $S(\Sigma_S) = S(\Sigma'_S) \Leftrightarrow (\Sigma_S \cong \Sigma'_S)$ и $S(\Sigma_S) = S(\Sigma'_S) \Rightarrow (\Sigma_S \approx \Sigma'_S)$.

Определение 4. Будем говорить, что ГКП $G = <Y, Q, Z, K, \psi, \varphi>$ *неотличим* от ГКП $G' = <Y, Q', Z, K, \psi', \varphi'>$, если его проекция G_k на любом ключе $k \in K$ сильно неотличима [5] от аналогичной проекции G'_k автомата G', т. е. каждое состояние в G_k неотличимо от некоторого состояния в G'_k.

Теорема 3. 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 $G = <Y, Q, Z, K, \psi, \varphi>$, $G' = <Y, Q', Z, K, \psi', \varphi'>$. 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

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

$\bar{e}'(q'_0, x_0x_1\ldots x_{n-1}, k) = y'_0y'_1\ldots y'_{n-1}$, где $\begin{cases} z'_t = \varphi'_k(q'_t), \\ y'_t = e'(x_t, z'_t), \\ q'_{t+1} = \psi'_k(y'_t, q'_t), \end{cases} \quad t = 0, 1, \ldots, n-1.$

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

База индукции: $t = 0$. Имеем: $z_0 = \varphi_k(q_0) = \varphi'_k(q'_0) = z'_0$, $y_0 = e(x_0, z_0) = e(x_0, z'_0) = y'_0$.

Предположение индукции: $y_0y_1\ldots y_{t-1} = y'_0y'_1\ldots y'_{t-1}$ для некоторого t, $n > t \geqslant 1$.

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

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

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

Ввиду произвольности $k \in K$, $q_0 \in Q$, $\alpha \in X^*$ и определения 3 теорема доказана. ■

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

6.3. Автоматные шифрсистемы

Определение 5. Назовём *автоматной шифрсистемой* пятерку объектов $\Sigma_A = <X, Y, K, E, D>$, где $E = <X, Q, Y, K, \psi, \varphi>$ и $D = <Y, Q^*, X, K, \psi^*, \varphi^*>$ суть свободно инициализируемые криптоавтоматы, 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

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

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

Теорема 4. Функция выходов автомата шифрования автоматной шифрсистемы при любых фиксированных значениях состояния и ключа инъективна как функция одного аргумента — входного символа.

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

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

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

Выше, в разд. 5.1 и 5.2, мы видели, что в самых первых шифрах на основе конечных автоматов (пурпурная машина и шифр Закревского) использовались обратимые автоматы с функциями выходов, биективными в каждом состоянии. Теорема 4 говорит о том, что других обратимых автоматов не бывает. Вместе с тем ниже (в разд. 7) мы увидим, что конечно-автоматные шифры можно строить и на автоматах, обратимых с конечной задержкой, в которых функция выходов не обязана быть инъективной по входной переменной.

6.4. Равносильность поточных и автоматных шифрсистем

Определение 6. Две шифрсистемы (поточные или автоматные) называются *эквивалентными*, если они задают одно и то же семейство последовательностных шифров (в предположении о равенстве последних с одной и той же функцией шифрования). Два класса шифрсистем (поточных или автоматных) *равносильны*, если каждая шифрсистема любого из них эквивалентна некоторой шифрсистеме другого.

Теорема 5. 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 $G = <Y, Q', Z, K, \psi', \varphi'>$, и построим автоматную шифрсистему $\Sigma_A = <X, Y, K, E, D>$, где криптоавтоматы $E = <X, Q, Y, K, \psi, \varphi>$ и $D = <Y, Q^*, X, K, \psi^*, \varphi^*>$ определяются соотношениями

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

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

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

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 $E = <X, Q, Y, K, \psi, \varphi>$ и $D = <Y, Q^*, X, K, \psi^*, \varphi^*>$, и построим поточную шифрсистему $\Sigma_S = <X, Y, K, G, e, d>$, где операции e, d и криптоавтомат $G = <Y, Q', Z, K, \psi', \varphi'>$ определяются соотношениями

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

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

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

где функция $\varphi^{-1}_{qk}(y)$ является обратной к функции $\varphi_{qk}(x)$. Она существует в силу инъективности последней по теореме 4.

Непосредственно проверяется, что

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

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

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. ■

6.5. Самосинхронизирующиеся поточные шифрсистемы

Определение 7. Назовём автомат $A = <X, Q, Y, \psi, \varphi>$ *самосинхронизирующимся с задержкой* τ, если выполняется условие

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

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, последующим входным словом ξ и, может быть, начальным состоянием q». Иначе говоря, происходит следующее: автомат словами α или α' переводится из состояния q в состояние $\psi(\alpha, q)$ или $\psi(\alpha', q)$ соответственно; затем словом $\tilde{\alpha}$ длиной τ — в состояние $\psi(\tilde{\alpha}, \psi(\alpha, q)) = \psi(\alpha\tilde{\alpha}, q)$ или $\psi(\alpha'\tilde{\alpha}, q)$ соответственно; после этого он будет вести себя одинаково в обоих случаях (выдавая на входную последовательность ξ одну и ту же выходную), т. е. синхронизируется словом $\tilde{\alpha}$.

Определение 8. 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 9 (конструктивное). 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 криптоавтомата G является самосинхронизирующимся автоматом с задержкой τ.

Определение 10 (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 Z любой рассматриваемой поточной шифрсистемы Σ_S нет различных эквивалентных символов, т. е. таких z и z', что $z \neq z'$, но $\forall x \in X[e(x, z) = e(x, z')]$ и $\forall y \in Y[d(y, z) = d(y, z')]$. 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 6. 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 $G = <Y, Q, Z, K, \psi, \varphi>$. 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 криптоавтомата G является самосинхронизирующимся автоматом с задержкой τ».

Используем 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 $q_\tau = \psi_k(\beta\tilde{\beta}, q)$, $q'_\tau = \psi_k(\beta'\tilde{\beta}, q)$, $\gamma = z_\tau z_{\tau+1}\dots z_{l-1} = \bar{\varphi}_k(\zeta, q_\tau) = \bar{\varphi}_k(\zeta, \psi_k(\beta\tilde{\beta}, q))$ и $\gamma' = z'_\tau z'_{\tau+1}\dots z'_{l-1} = \bar{\varphi}_k(\zeta, q'_\tau) = \bar{\varphi}_k(\zeta, \psi_k(\beta'\tilde{\beta}, q))$. В силу (К) имеет место $\bar{\varphi}_k(\zeta, \psi_k(\beta\tilde{\beta}, q)) = \bar{\varphi}_k(\zeta, \psi_k(\beta'\tilde{\beta}, q))$, поэтому $\gamma = \gamma'$ и $x_i = d(y_i, z_i) = d(y_i, z'_i) = x'_i$ 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,

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

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

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 $z_t = \varphi_k(y_t, \psi_k(\beta_0\tilde{\beta}_0, q)) \neq \varphi_k(y_t, \psi_k(\beta'_0\tilde{\beta}_0, q)) = z'_t$, или с учётом того, что G_k является автоматом Мура, $z_t = \varphi_k(q_t) \neq \varphi_k(q'_t) = z'_t$ для $q_t = \psi_k(\beta_0\tilde{\beta}_0, q)$ и $q'_t = \psi_k(\beta'_0\tilde{\beta}_0, q)$.

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 $x = d(y, \varphi_k(q_t)) = d(y, z_t)$ и $x' = d(y, \varphi_k(q'_t)) = d(y, z'_t)$, а в силу (Д) $x = x'$. Таким образом, $\forall y \in Y(d(y, z_t) = d(y, z'_t))$, откуда ввиду взаимной обратимости d и e следует $\forall x \in X(e(x, z_t) = e(x, z'_t))$, что противоречит отсутствию в Z эквивалентных символов. ■

6.6. Регистровость самосинхронизирующихся конечных автоматов

Определение 11. Назовём автомат Мура $R = <Y, Y^\tau, Z, \sigma, \rho>$ *регистром сдвига длиной* τ, если его функция переходов σ есть функция сдвига, определяемая для $\tilde{\beta} = y_1 y_2 \dots y_\tau \in Y^\tau$ и $y \in Y$ как $\sigma(y, \tilde{\beta}) = y_2 \dots y_\tau y$.

Теорема 7. Всякий сильносвязный самосинхронизирующийся с задержкой τ автомат Мура $G = <Y, Q, Z, \psi, \varphi>$ эквивалентен некоторому регистру сдвига $R = <Y, Y^\tau, Z, \sigma, \rho>$ длиной τ.

Доказательство. Требуется построить функцию выходов ρ регистра R со следующим свойством:

$$\forall q \in Q \exists \tilde{\alpha} \in Y^\tau \forall \beta \in Y^* [\bar{\varphi}(\beta, q) = \bar{\rho}(\beta, \tilde{\alpha})].$$

Ввиду самосинхронизируемости с задержкой τ автомата G

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

откуда при $\zeta = \Lambda$

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

Ввиду сильной связности G для любых $q, s \in Q$ существует $\gamma \in Y^*$, что $\psi(\gamma, q) = s$. Положим $\beta = \Lambda$, $\beta' = \gamma$. Тогда

$$\forall q \in Q \forall \tilde{\beta} \in Y^\tau [\varphi(\psi(\tilde{\beta}, q)) = \varphi(\psi(\gamma\tilde{\beta}, q))],$$

а так как $\varphi(\psi(\tilde{\beta}, q)) = \varphi(\tilde{\beta}, q)$ и $\varphi(\psi(\gamma\tilde{\beta}, q)) = \varphi(\psi(\tilde{\beta}, \psi(\gamma, q))) = \varphi(\psi(\tilde{\beta}, s)) = \varphi(\tilde{\beta}, s)$, то $\forall q, s \in Q \forall \tilde{\beta} \in Y^\tau [\varphi(\tilde{\beta}, q) = \varphi(\tilde{\beta}, s)]$. Последнее означает, что в G значение $\varphi(\tilde{\beta}, q)$ в действительности не зависит от состояния q, и можно ределить функцию $\rho\colon Y^\tau \to Z$ как $\rho(\tilde{\beta}) = \varphi(\tilde{\beta}, q)$ для любого $\tilde{\beta} \in Y^\tau$ и некоторого (любого) $q \in Q$.

Кроме того, из сильной связности G следует существование для каждого $q \in Q$ такого $\beta'\tilde{\beta} \in Y^*$, что $|\tilde{\beta}| = \tau$ и $\psi(\beta'\tilde{\beta}, q) = q$. Определённое так для $q \in Q$ некоторое слово $\tilde{\beta} \in Y^\tau$ и рассматриваемое как состояние требуемого регистра R обозначим $\tilde{\beta}_q$.

Теперь для доказательства теоремы достаточно показать, что для любых $q \in Q$ и $\beta \in Y^*$ выполняется равенство $\bar{\varphi}(\beta, q) = \bar{\rho}(\beta, \tilde{\beta}_q)$. Сделаем это индукцией по длине слова $\beta \in Y^*$. Пусть $q \in Q$ и $\tilde{\beta}_q = \tilde{\alpha}$. Тогда $q = \psi(\beta'\tilde{\alpha}, q)$ для некоторого $\beta' \in Y^*$.

База индукции: $\beta = \Lambda$. Имеем: $\bar{\varphi}(\Lambda, q) = \varphi(q) = \varphi(\psi(\beta'\tilde{\alpha}, q)) = \varphi(\tilde{\alpha}, \psi(\beta', q)) = \rho(\tilde{\alpha}) = \bar{\rho}(\Lambda, \tilde{\alpha}) = \bar{\rho}(\Lambda, \tilde{\beta}_q)$.

Предположение индукции: $\bar{\varphi}(\beta, q) = \bar{\rho}(\beta, \tilde{\beta}_q)$ для некоторого $\beta \in Y^*$.

Шаг индуции. Пусть $y \in Y$. Покажем, что $\bar{\varphi}(\beta y, q) = \bar{\rho}(\beta y, \tilde{\beta}_q)$. Положим $\delta\tilde{\beta} = \beta'\tilde{\alpha}\beta y$, где $|\tilde{\beta}| = \tau$. Тогда, ввиду определения функции сдвига, $\tilde{\beta} = \sigma(\delta\tilde{\beta}, \tilde{\beta}_q)$ и $\varphi(\beta y, q) = \varphi(\psi(\beta y, q)) = \varphi(\psi(\beta y, \psi(\beta'\tilde{\alpha}, q))) = \varphi(\psi(\beta'\tilde{\alpha}\beta y, q)) = \varphi(\psi(\delta\tilde{\beta}, q)) = \varphi(\psi(\tilde{\beta}, \psi(\delta, q))) = \varphi(\tilde{\beta}, \psi(\delta, q)) = \rho(\tilde{\beta}) = \rho(\sigma(\delta\tilde{\beta}, \tilde{\beta}_q)) = \rho(\sigma(\beta'\tilde{\alpha}\beta y, \tilde{\beta}_q)) = \rho(\sigma(\beta y, \sigma(\beta'\tilde{\alpha}, \tilde{\beta}_q))) = \rho(\sigma(\beta y, \tilde{\alpha})) = \rho(\beta y, \tilde{\beta}_q)$. Поэтому $\bar{\varphi}(\beta y, q) = \bar{\varphi}(\beta, q)\varphi(\beta y, q) = \rho(\beta, \tilde{\beta}_q)\rho(\beta y, \tilde{\beta}_q) = \bar{\rho}(\beta y, \tilde{\beta}_q)$, и шаг индукции доказан. ■

6.7. Регистровые шифрсистемы

Определение 12. Назовём *регистром сдвига длиной τ с ключом* такой свободно инициируемый криптоавтомат $R = <Y, Y^\tau, Z, K, \sigma, \rho>$, что для любого значения $k \in K$ его проекция $R_k = <Y, Y^\tau, Z, \sigma_k, \rho_k>$ есть регистр сдвига длиной τ.

Определение 13. 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 алгоритм шифрования $\bar{e}$ можно переписать в более простой форме:

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

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

Эти уравнения проиллюстрированы схемой на рис. 4.

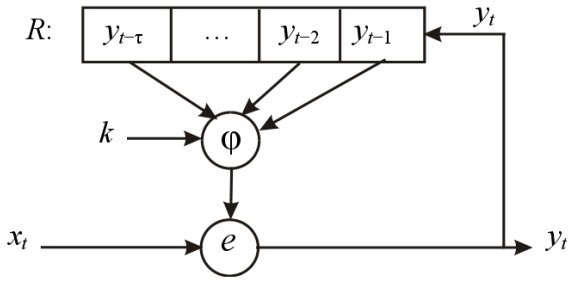

Рис. 4. Схема регистровой шифрсистемы

Регистровая шифрсистема размерности τ является самосинхронизирующейся с задержкой τ по конструктивному определению. Ниже показывается, что в некоторой степени справедливо и обратное.

6.8. Регистровость самосинхронизирующихся поточных шифрсистем

Теорема 8. Любая самосинхронизирующаяся с задержкой τ поточная шифрсистема $\Sigma_S = <X, Y, K, G, e, d>$, у которой все проекции G_k ГКП G суть сильносвязные автоматы, неотличима от некоторой регистровой шифрсистемы $\Sigma_R = <X, Y, K, R, e, d>$ размерности τ.

Доказательство. Пусть $G = <Y, Q, Z, K, \psi, \varphi>$, $k \in K$ и $G_k = <Y, Q, Z, \psi_k, \varphi_k>$. По конструктивному определению самосинхронизирующейся системы Σ_S следует, что G_k есть сильносвязный самосинхронизирующийся автомат с задержкой τ. По теореме 7 для него можно построить сильно неотличимый регистр сдвига $R_k = <Y, Y^\tau, Z, \sigma, \rho_k>$ длиной τ. Возьмём функцию $\varphi\colon K \times Y \times Y^\tau \to Z$, такую, что $\varphi(k, y, \tilde{\beta}) = \rho_k(\tilde{\beta})$, и следовательно, зависящую от аргумента $y \in Y$ фиктивно. Построим регистр сдвига с ключом $R = <Y, Y^\tau, Z, K, \sigma, \varphi>$ и регистровую шифрсистему $\Sigma_R = <X, Y, K, R, e, d>$ с регистром R в качестве ГКП.

По построению для любого ключа $k \in K$ регистр R_k является проекцией регистра R и автомат G_k сильно неотличим от R_k. По определению 4 ГКП G неотличим

от регистра R. Следовательно, по теореме 3 поточная шифрсистема Σ_S неотличима от регистровой шифрсистемы Σ_R размерности τ. ■

Заметим, что в [6] под самосинхронизирующимися поточными шифрами понимаются именно регистровые шифрсистемы. Теорема 8 служит по существу теоретическим обоснованием такого понимания.

6.9. Самосинхронизирующиеся автоматные шифрсистемы

Определение 14. Назовём автоматную шифрсистему $\Sigma_A = <X, Y, K, E, D>$ *самосинхронизирующейся с задержкой* τ, если для её автомата расшифрования $D = <Y, Q^*, X, K, \psi^*, \varphi^*>$ выполняется следующее условие:

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

Из определений 5, 8 и 14 непосредственно следует, что автоматная шифрсистема является самосинхронизирующейся с задержкой τ, если и только если этим свойством обладают все задаваемые ею последовательностные шифры.

Теорема 9. Любая самосинхронизирующаяся с задержкой τ автоматная шифрсистема $\Sigma_A = <X, Y, K, E, D>$, у которой для каждого $k \in K$ проекция E_k шифрующего автомата $E = <X, Q, Y, K, \psi, \varphi>$ является сильносвязным автоматом, неотличима от некоторой регистровой шифрсистемы $\Sigma_R = <X, K, Y, R, e, d>$ размерности τ.

Доказательство. Следуя доказательству теоремы 5, построим поточную шифрсистему $\Sigma_S = <X, Y, K, G, e, d>$, эквивалентную шифрсистеме Σ_A. Поскольку шифрсистемы Σ_A и Σ_S эквивалентны и шифрсистема Σ_A является самосинхронизирующейся с задержкой τ, то шифрсистема Σ_S также является самосинхронизирующейся с задержкой τ.

Пусть $E = <X, Q, Y, K, \psi, \varphi>$ и $G = <Y, Q, Z, K, \psi', \varphi'>$. Зафиксируем любое значение ключа $k \in K$ и рассмотрим в Σ_S проекцию G_k криптоавтомата G. По построению в доказательстве теоремы 5 функция переходов ГКП G определяется как

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

Соответственно этому функция переходов его проекции G_k определится как

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

Поскольку по теореме 4 функция φ_{qk} инъективна, то обратная ей функция φ_{qk}^{-1} существует и сюрьективна. В этом случае для любых $q_1, q_2 \in Q$, $\alpha \in X^*$, $\beta \in Y^*$ если $\psi_k(\alpha, q_1) = q_2$ и $\bar{\varphi}_k(\alpha, q_1) = \beta$, то $\bar{\varphi}_k^{-1}(\beta, q_1) = \alpha$ и $\psi'_k(\beta, q_1) = \psi_k(\bar{\varphi}_{qk}^{-1}(\beta), q_1) = \psi_k(\alpha, q_1) = q_2$, и из сильной связности автомата E_k следует сильная связность автомата G_k. Теперь по теореме 8 шифрсистема Σ_S, а вместе с ней и шифрсистема Σ_A, неотличима от некоторой регистровой шифрсистемы $\Sigma_R = <X, Y, K, R, e, d>$ размерности τ. ■

7. Конечно-автоматные криптосистемы с открытым ключом

7.1. Введение

Рассмотрим класс конечно-автоматных криптосистем с открытым ключом, известных под сокращённым названием FAPKC — Finite Automaton Public Key Cryptosystems [20]. В основе их теории лежит понятие автомата, слабо обратимого с конечной задержкой τ. Так называется конечный автомат, в котором любое слово во входной

последовательности однозначно определяется по соответствующим начальному состоянию и слову выходной последовательности и по следующим за этим словом τ выходным символам. Иначе говоря, входная информация автомата восстанавливается по выходной с задержкой на τ тактов работы автомата, и эту операцию может выполнить другой автомат, называемый обратным к первому.

В любой FAPKC закрытый ключ состоит из двух слабо обратимых автоматов, обратные к которым могут быть легко (с полиномиальной сложностью) построены, а открытый ключ представляет собой последовательную композицию автоматов в закрытом ключе, обратный к которой автомат легко строится по автоматам, обратным к её компонентам. Криптосистема может быть использована как для шифрования (открытым ключом) и расшифрования (автоматом, обратным к открытому ключу), так и для подписания (этим автоматом) и для проверки подписи (открытым ключом). Предполагая, что хотя бы одна из компонент в композиции нелинейная, ожидается, что декомпозиция открытого ключа — с целью получения его закрытых компонент и построение автомата, обратного к открытому ключу, — с целью дешифрования и подписания без знания закрытого ключа являются трудными задачами (экспоненциальной сложности). Следовательно, любой пользователь криптосистемы может зашифровывать сообщения или проверять подписи, используя открытый ключ, но не может ни дешифровать криптограммы, ни подделать подписи без знания двух закрытых компонент. Чтобы скрыть эти компоненты от их прочтения из открытой композиции, предполагается последнюю выражать системой булевых функций, и тогда возникает проблема обеспечения умеренного размера открытого ключа, так как размер системы булевых функций композиции с нелинейной выходной компонентой может достигать неприемлемо больших размеров.

В этом разделе после введения необходимых элементов теории автоматов описывается общая схема построения FAPKC, указываются параметры некоторых версий FAPKC и в качестве примера приводится описание простейшей из них. Весь материал в нём, кроме примера, излагается по статье [20]. Изложение ведётся в стиле и обозначениях, единых для всех разделов.

7.2. Обратимость автоматов

Пусть τ является целым неотрицательным числом. Конечный автомат $M = <X, Q, Y, \psi, \varphi>$ называется *слабо обратимым с задержкой* τ, если

$$\forall q \in Q \forall \delta, \varepsilon \in X^\tau \forall a, b \in X (a \neq b \Rightarrow \bar{\varphi}(a\delta, q) \neq \bar{\varphi}(b\varepsilon, q).$$

Наименьшее такое τ обозначается $\tau(M)$. Поскольку других типов обратимости здесь мы не рассматриваем, то всюду далее наречие «слабо» и производные от него прилагательные в соответствующем контексте опускаются. Автомат, обратимый с некоторой задержкой $\tau \geqslant 0$, называется *обратимым* автоматом. Автомат $M' = <Y, Q', X, \psi', \varphi'>$ называется *обратным с задержкой* τ *к автомату* M, если

$$\forall q \in Q \exists q' \in Q' \forall \alpha \in X^* \forall \delta \in X^\tau \exists \varepsilon \in X^\tau (\bar{\varphi}'(\bar{\varphi}(\alpha\delta, q), q') = \varepsilon\alpha);$$

в этом случае q' называется τ-*соответствующим состоянию* q, а пара (q, q') — τ-*парой* в $M \times M'$. Автомат, обратный к автомату M с некоторой задержкой, называется *обратным к* M.

7.3. Композиция автоматов

(*Последовательной*) *композицией* конечных автоматов $M_1 = <X, Q_1, Y, \psi_1, \varphi_1>$ и $M_2 = <Y, Q_2, Z, \psi_2, \varphi_2>$ называется автомат $M_1 \times M_2 = <X, Q_1 \times Q_2, Z, \psi, \varphi>$, в котором

для любых $x \in X$, $q_1 \in Q_1$ и $q_2 \in Q_2$

$$\varphi(x, q_1q_2) = \varphi_2(\varphi_1(x, q_1), q_2) \text{ и } \psi(x, q_1q_2) = (\psi_1(x, q_1), \psi_2(\varphi_1(x, q_1), q_2));$$

в этом случае M_1 и M_2 называются соответственно *первой* и *второй компонентами* в композиции $M_1 \times M_2$.

7.4. Автоматы с конечной памятью

Автомат M называется автоматом *с конечной памятью*, если $Q = X^h \times Y^k$ для некоторых целых $h, k \geqslant 0$ и всех $(x_{-h} \dots x_{-1}x_0) \in X^{h+1}$ и $(y_{-k}y_{-k+1} \dots y_{-1}) \in Y^k$

$$\begin{gathered}\psi(x_0, x_{-h}x_{-h+1} \dots x_{-1}y_{-k}y_{-k+1} \dots y_{-1}) = \\ = (x_{-h+1} \dots x_{-1}x_0y_{-k+1} \dots y_{-2}y_{-1}\varphi(x_0, x_{-h}x_{-h+1} \dots x_{-1}y_{-k}y_{-k+1} \dots y_{-1}));\end{gathered} \tag{1}$$

в этом случае числа $\mu(M) = \max(h, k)$, h и k называются соответственно *памятью*, *входной* и *выходной памятью* автомата M, а функция $f\colon X^{h+1} \times Y^k \to Y$, определяемая для всех $(x_{-h} \dots x_{-1}x_0) \in X^{h+1}$ и $(y_{-k}y_{-k+1} \dots y_{-1}) \in Y^k$ как

$$f(x_{-h} \dots x_{-1}x_0y_{-k}y_{-k+1} \dots y_{-1}) = \varphi(x_0, x_{-h}x_{-h+1} \dots x_{-1}y_{-k}y_{-k+1} \dots y_{-1}), \tag{2}$$

— *входо-выходной функцией* автомата M. Непосредственно проверяется, что в таком автомате для любого $t \geqslant 0$ и для любых $q \in Q$ и $x_0x_1 \dots x_t \in X^{t+1}$ имеет место

$$\varphi(x_0x_1 \dots x_t, q) = f(x_{t-h}x_{t-h+1} \dots x_t\bar{\varphi}(x_{t-k}x_{t-k+1} \dots x_{t-1}, \psi(x_0x_1 \dots x_{t-k-1}, q))),$$

т. е. в любой момент времени $t \geqslant 0$ выходной символ $y_t = \varphi(x_0x_1 \dots x_t, q)$ автомата с конечной памятью вычисляется как значение его входо-выходной функции f от входных символов $x_{t-h}, x_{t-h+1}, \dots, x_t$ в этот и предыдущие h моментов времени и от набора $y_{t-k}y_{t-k+1} \dots y_{t-1} = \bar{\varphi}(x_{t-k}x_{t-k+1} \dots x_{t-1}, \psi(x_0x_1 \dots x_{t-k-1}, q))$ выходных символов в предыдущие k моментов времени:

$$y_t = f(x_{t-h}x_{t-h+1} \dots x_ty_{t-k}y_{t-k+1} \dots y_{t-1}),\ t = 0, 1, \dots \tag{3}$$

Уравнения (3) называются далее входо-выходными уравнениями автомата M. Выражение в правой части уравнения для $t = 0$ в них является выражением для f.

Соотношениями (1) и (2) функции ψ и φ определяются однозначно по f. Это значит, что автомат M с конечной памятью может быть задан его входо-выходной функцией f или входо-выходными уравнениями. В дальнейшем, где это не вызывает двусмысленности, мы пользуемся этой возможностью без дополнительных оговорок, отождествляя такой автомат M с его входо-выходной функцией f или обозначая его как $M_f = <X, Q_f, Y, \psi_f, \varphi_f>$. Полагаем, в частности, $\mu(f) = \mu(M)$. Кроме того, в случае надобности указать параметры автомата f, последний записывается как $<X, Y, h, k, f>$.

7.5. Автоматы с входной памятью

Автомат с конечной памятью $<X, Y, h, k, f>$ называется автоматом *с входной памятью* h, если его выходная память равна 0, т. е. если $\mu(f) = h$ и, следовательно, его входо-выходная функция является отображением $f\colon X^{h+1} \to Y$. Входо-выходные уравнения для него имеют вид

$$y_t = f(x_{t-h}x_{t-h+1} \dots x_t),\ t = 0, 1, \dots \tag{4}$$

Произведением автоматов $f_1\colon X^{h+1} \to Y$ и $f_2\colon Y^{h'+1} \to Z$ называется автомат $f_1f_2\colon X^{h+h'+1} \to Z$, в котором для любого набора $\alpha = x_{-h-h'}x_{-h-h'+1} \dots x_0 \in X^{h+h'+1}$

$$f_1f_2(\alpha) = f_2(f_1(x_{-h-h'}x_{-h-h'+1} \dots x_{-h'})f_1(x_{-h'-h+1}x_{-h'-h+2} \dots x_{-h'-1}) \dots f_1(x_{-h}x_{-h+1} \dots x_0)).$$

Теорема 10. Произведение $f_1 f_2$ и композиция $f_1 \times f_2$ автоматов f_1 и f_2 с входной памятью находятся в следующем отношении между собой [21]: любое состояние $q = (x_{-h-h'} \dots x_{-2} x_{-1}) \in X^{h+h'} = Q_{f_1 f_2}$ эквивалентно состоянию $(q_1, q_2) \in Q_{f_1} \times Q_{f_2}$, где

$$q_1 = (x_{-h} \dots x_{-2} x_{-1}) \in X^h = Q_{f_1},$$

$$q_2 = \bar{\varphi}_{f_1}(x_{-h'} \dots x_{-2} x_{-1}, x_{-h-h'} \dots x_{-h'-2} x_{-h'-1}) \in X^{h'} = Q_{f_2}.$$

Теорема 11. Автомат $f\colon X^{h+1} \to X$ обратим с задержкой τ, если и только если $\forall q \in Q_f (\bar{\varphi}_f(X^{\tau+1}, q) = \bar{\varphi}_f(X^\tau, q) \times X)$, где $\forall k \geqslant 1 (\bar{\varphi}_f(X^k, q) = \{\bar{\varphi}_f(\alpha, q)\colon \alpha \in X^k\})$.

Теорема 12. Пусть автомат $f = f\colon X^{h+1} \to X$ обратим, автомат $M' = <X, Q', X, \psi', \varphi'>$ обратен к M_f с задержкой τ и (q, q') является τ-парой в $M_f \times M'$. Тогда M_f обратен к M' с задержкой τ и τ-парой в $M' \times M_f$ является (q'_1, q), где $q'_1 = \psi'(\bar{\varphi}_f(\xi, q), q')$ для произвольного $\xi \in X^\tau$.

Теорема 13. Пусть автомат $f = f\colon X^{h+1} \to X$ обратим, $\tau(f) = \tau$, автомат $M' = <X, Q', X, \psi', \varphi'>$ обратен к M_f с задержкой τ', (q, q') является τ'-парой в $M_f \times M'$, $\alpha = a_0 a_1 \dots a_{n-1+\tau}$, $\beta = b_0 b_1 \dots b_{n-1+\tau} \in X^{n+\tau}$, $n \geqslant 0$. Тогда уравнение $\bar{\varphi}_f(\alpha, q) = \beta$ разрешимо относительно α, если и только если $b_0 b_1 \dots b_{\tau-1} \in \bar{\varphi}_f(X^\tau, q)$; в этом случае слово $a_0 a_1 \dots a_{n-1}$ определяется обнозначно и $\bar{\varphi}'(\beta\zeta, q') = \xi\alpha$ для любого $\zeta \in X^{\tau'}$ и некоторого $\xi \in X^{\tau'}$.

Теорема 14. Для автоматов $f_1,\ f_2$ с входной памятью автомат $f = f_1 f_2$ обратим, если и только если обратим каждый из автоматов $f_1,\ f_2$; в этом случае

$$\tau(f_i) \leqslant \tau(f) \leqslant \tau(f_1) + \tau(f_2), \quad i = 1, 2.$$

Теорема 15. Пусть автомат $f = f\colon X^{h+1} \to X$ обратим, $\tau(f) \leqslant \tau$, $Q_f = X^h$, $s \in X^{h-\tau}$, $\alpha, \beta \in X^n$, $\xi \in X^\tau$. Тогда уравнение $\bar{\varphi}_f(\alpha, s\xi) = \beta$ всегда имеет решение $\xi\alpha \in X^{\tau+n}$. Более того, слово $\xi\alpha \in X^{\tau+n}$ есть решение, если и только если $\bar{\varphi}_f(\xi\alpha, as) = b\beta$ для некоторых $a \in X^\tau$, $b \in \bar{\varphi}_f(X^\tau, as)$.

Теорема 16. Пусть $f = f_1 f_2$ и состояние $q \in Q_f$ эквивалентно состоянию $(q_1, q_2) \in Q_{f_1} \times Q_{f_2}$. Пусть также автомат M'_2 обратен к M_{f_2} с задержкой τ_2, φ'_2 — его функция выходов и (q_2, q'_2) является τ_2-парой в $M_{f_2} \times M'_2$. Тогда α есть решение уравнения $\bar{\varphi}_f(\alpha, q) = \beta$, если и только если $\bar{\varphi}_{f_1}(\alpha, q_1) = \beta'$, где $\zeta\beta' = \bar{\varphi'}_2(\beta\xi, q'_2)$ для произвольного $\xi \in X^{\tau_2}$ и некоторого $\zeta \in X^{\tau_2}$.

Теорема 17. Пусть автомат $M' = <X, Q', X, \psi', \varphi'>$ обратен с задержкой τ к автомату f и (s, s') есть некоторая τ-пара в $M_f \times M'$. Тогда для любого состояния $q \in Q_f$ в M_f также τ-парой в $M_f \times M'$ будет (q, q'), где $q' = \psi'(\bar{\varphi}_f(\xi q, s), s')$ для произвольного $\xi \in X^d$, где $d = 0$, если $h \geqslant \tau$, и $d = \tau - h$, если $\tau > h$.

Пусть далее для любого автомата $M = <X, Q, Y, \psi, \varphi>$ и любого целого $\tau \geqslant 0$ автомат $M^{(\tau)} = <X, Q \times \{0, 1, \dots, \tau\}, Y, \psi^{(\tau)}, \varphi^{(\tau)}>$ определяется как

$$\psi^{(\tau)}(x, (q, i)) = \begin{cases} (q, i+1), & 0 \leqslant i < \tau, \\ (\psi(x, q), \tau), & i = \tau, \end{cases} \quad \varphi^{(\tau)}(x, (q, i)) = \begin{cases} y_0, & 0 \leqslant i < \tau, \\ \varphi(x, q), & i = \tau \end{cases}$$

для некоторого $y_0 \in Y$.

Теорема 18. Пусть $f_1,\ f_2$ — обратимые автоматы с входной памятью, $f = f_1 f_2$ и M'_i для $i = 1, 2$ есть автомат, обратный к автомату M_{f_i} с задержкой τ_i. Тогда автомат $M' = M'_2 \times M_1'^{(\tau_2)}$ является обратным с задержкой $\tau = \tau_1 + \tau_2$ к автомату M_f. Более того, пусть для произвольного состояния q автомата M_f пара (q_1, q_2) обозначает состояние автомата $M = M_{f_1} \times M_{f_2}$, которое по теореме 10 эквивалентно q, и пусть (q_i, q'_i) есть τ_i-пара в $M_{f_i} \times M'_i$, $i = 1, 2$. Тогда $(q, (q'_2, (q'_1, 0)))$ есть τ-пара в $M_f \times M'$.

Следствие 1. В условиях теоремы если каждое состояние в M эквивалентно некоторому состоянию в M_f, то автомат M' обратен к автомату M с задержкой τ и $((q_1, q_2), (q'_2, (q'_1, 0)))$ является τ-парой в $M \times M'$.

7.6. Автоматы с конечной памятью над конечным полем

Пусть F есть конечное поле, в частности $F = GF(2)$, и $l, m \geqslant 1$. Предполагается, что элементы в F^l и F^m записываются как вектор-столбцы. Будем рассматривать автоматы с конечной памятью $f\colon X^{h+1} \times Y^k \to Y$, в которых $X = F^l$, $Y = F^m$, и называть их автоматами над полем F или в алфавите F^l, если $m = l$. Их множество обозначаем $\Upsilon_{l,m}(F)$.

Множество всех матриц размера $m \times l$ над любым кольцом R обозначается $M_{m,l}(R)$. Тем самым определены, в частности, $M_{m,l}(F[z])$ и $M_{m,l}(F)$ — множества всех матриц размера $m \times l$ над кольцом многочленов $F[z]$ и над полем F соответственно.

Автомат f над F называется *разделимым*, или автоматом *с разделимой памятью*, если для некоторых функций $f_1\colon X^{h+1} \to Y$ и $f_2\colon Y^k \to Y$, называемых *компонентами разделимости*, и для любых наборов $(x_{-h} \dots x_{-1}x_0) \in X^{h+1}$ и $(y_{-k}y_{-k+1} \dots y_{-1}) \in Y^k$

$$f(x_{-h} \dots x_{-1}x_0 y_{-k}y_{-k+1} \dots y_{-1}) = f_1(x_{-h} \dots x_{-1}x_0) + f_2(y_{-k}y_{-k+1} \dots y_{-1});$$

в этом случае автомат M_f обозначается как M_{f_1,f_2}.

Непосредственно проверяется, что автомат M_{f_1,f_2} в алфавите F^l обратим с задержкой τ, если и только если таковым является автомат M_{f_1}.

Если в автомате $M_f = M_{f_1,f_2}$

$$f_1(x_{-h} \dots x_{-1}x_0) = \sum_{j=0}^{h} A_j x_{-h+j}, \quad f_2(y_{-k}y_{-k+1} \dots y_{-1}) = \sum_{j=1}^{k} B_j y_{-k+j},$$

где $A_0, A_1, \dots, A_h$ и $B_1, B_2, \dots, B_k$ суть матрицы в $M_{m,l}(F)$ и $M_{m,m}(F)$ соответственно, то автомат M_f называется *линейным*.

7.7. Автоматы с входной памятью над конечным полем

По определению, автомат над полем F с входной памятью h, с размерностью входа l и с размерностью выхода m задаётся как $f\colon X^{h+1} \to Y$, или как $M_f = <X, Q_f, Y, \psi_f, \varphi_f>$, где $X = F^l$, $Y = F^m$, $Q_f = X^h$, $\psi_f(x_0, x_{-h}x_{-h+1} \dots x_{-1}) = x_{-h+1} \dots x_{-1}x_0$, $\varphi_f(x_0, x_{-h}x_{-h+1} \dots x_{-1}) = f(x_{-h} \dots x_{-1}x_0)$. Множество всех таких автоматов обозначается $\Im_{l,m}(F)$, а тех из них, которые обратимы, — $\Im'_{l,m}(F)$. В линейном автомате $f \in \Im_{l,m}(F)$ имеем $f(x_{-h} \dots x_{-1}x_0) = \sum_{j=0}^{h} A_j x_{-h+j}$ для некоторых матриц $A_0, A_1, \dots, A_h$ в $M_{m,l}(F)$. Множество всех линейных (обратимых) автоматов в $\Im_{l,m}(F)$ обозначается $\Im L_{l,m}(F)$ (соответственно $\Im' L_{l,m}(F)$).

Каждой матрице $A \in M_{m,l}(F[z])$ можно поставить во взаимно однозначное соответствие автомат $f \in \Im L_{l,m}(F)$ по следующему правилу. Пусть $A = \sum_{i=0}^{h} A_i z^i$ для некоторых матриц $A_0, A_1, \dots, A_h$ в $M_{m,l}(F)$. Последние находятся по A однозначно:

элемент в A_i для каждого $i = 0, 1, \ldots, h$ на пересечении строки a и столбца b равен коэффициенту при z^i в многочлене на пересечении строки a и столбца b в матрице A. Тогда $f(x_{-h} \ldots x_{-1}x_0) = \sum_{i=0}^{h} A_i x_{-i}$. Тем самым любой автомат в $\Im L_{l,m}(F)$ можно задать (отождествить с) соответствующей матрицей в $M_{m,l}(F[z])$. В дальнейшем, при необходимости, мы это делаем без дополнительных оговорок. В частности, автомат $f(x_{-h} \ldots x_{-1}x_0) = x_0$ задаётся тождественной матрицей I и записывается иногда как 1, а автомат $f(x_{-h} \ldots x_{-1}x_0) = x_i$ задаётся матрицей $z^i I$ и записывается иногда как z^i.

Матрицы в $M_{n,m}(F[z])$ можно умножать на автоматы в $\Im_{l,m}(F)$ для любых n, m, l. Так, всякий автомат $f = f(x_{-h} \ldots x_{-1}x_0)) \in \Im_{l,l}(F)$ может быть записан как $f = CT$, где $C \in M_{l,n}(F[z])$, $T = (T_1 T_2 \ldots T_n)^t \in \Im_{l,n}(F)$, t — оператор транспонирования и $T_1, \ldots, T_n$ суть некоторые различные мономы в переменных x_{-ij} для $i = 0, 1, \ldots, h$; $j = 1, 2, \ldots, l$. В случае $F = GF(2)$ это представление f называется *булевым выражением* для f.

Обозначим $GL_l(R)$ группу всех обратимых матриц размера $l \times l$ над кольцом R. Таким образом, определены группы $GL_l(F[z])$ и $GL_l(F)$. Любую ненулевую матрицу $B \in M_{l,l}(F[z])$ известным алгоритмом преобразования к диагональной форме можно разложить в произведение вида $B = PDQ(1 - zA)$, где $P \in GL_l(F[z])$, $Q \in GL_l(F)$, $A \in M_{l,l}(F[z])$ и $D = \mathrm{diag}(I_{n_0}, zI_{n_1}, \ldots, z^\tau I_{n_\tau}, 0_n)$ — диагональная матрица размера $l \times l$, где $n = l - \sum_{i=1}^{\tau} n_i$, $\tau \geqslant 0$, $n_\tau > 0$, $n_i \geqslant 0$ для $i < \tau$, I_{n_i} — тождественная матрица размера $n_i \times n_i$ и 0_n — нулевая матрица размера $n \times n$. Набор $(n_0, n_1, \ldots, n_\tau)$ определяется однозначно матрицей B и называется её *структурным параметром*. Число τ назовём длиной параметра.

Теорема 19. Пусть $B \in M_{l,l}(F[z])$, $B = PDQ(1 - zA)$ и τ — длина структурного параметра B. Тогда: 1) автомат B обратим, если и только если $\det(B) \neq 0$, или, равносильно, $l = \sum_{i=0}^{\tau} n_i$; в этом случае $\tau(B) = \tau$; 2) если $\tau(B) = \tau$, то автомат $M_{B',zA}$, где $B' = Q^{-1}CP^{-1}$ и $C = z^\tau D^{-1}$, обратен к автомату B и $(\underline{0}, (\underline{0}, \underline{0}))$ является τ-парой в $M_B \times M_{B',zA}$.

Теорема 20. Пусть $f = f(x_{-h} \ldots x_{-1}x_0) \in \Im_{l,l}(F)$. Тогда автомат f обратим с задержкой 0, если и только если $\varphi_{f_q} \colon X \to X$ является биекцией для каждого $q \in Q_f$; в этом случае $f(x_{-h} \ldots x_{-1}x_0) = \sum_{i=1}^{n} c_i(x_{-h} \ldots x_{-1}) P_i(x_0)$, где $n \geqslant 1$, P_i есть биекция на X, $c_i(x_{-h} \ldots x_{-1}) \in \{0, 1\}$, $0P_i(x_0) = 0$, $1P_i(x_0) = P_i(x_0)$ и $\sum_{i=1}^{n} c_i(x_{-h} \ldots x_{-1}) = 1$. Более того, пусть $f' = f'(x_0 y_{-h} \ldots y_{-1}) = \sum_{i=1}^{n} c_i(y_{-h} \ldots y_{-1}) P_i^{-1}(x_0)$. Тогда $M_{f'} \in \Upsilon_{l,l}(F)$, автомат $M_{f'}$ обратен к M_f с задержкой 0, $Q_{f'} = Q_f$ и (q, q) является 0-парой в $M_f \times M_{f'}$ для любого $q \in Q_f$. В частности, обратимы с задержкой 0 все автоматы следующих трёх типов: 1) биекции на X; 2) $1 + zg$ для любого $g \in \Im_{l,l}(F)$; 3) $1 + AgB$, где $A, B \in M_{l,l}(F[z])$, $AB = BA = 0$ и $g \in \Im_{l,l}(F)$.

Обозначим $\Im^\tau_{l,m}(F)$ множество всех автоматов в $\Im'_{l,m}(F)$, обратимых с задержкой τ. Следующий результат показывает, что множество $\Im^\tau_{l,l}(F)$ замкнуто относительно операции сложения с автоматами вида $z^{\tau+1}g$ для $g \in \Im_{l,l}(F)$. Для того чтобы увидеть, как обратный к $f + z^{\tau+1}g$ соотносится с обратным к f, определяется (*последовательная*) *композиция с обратной связью* автоматов M_β для $\beta \colon X^{h+1} \times Y^k \to Y$ и $M = <X, Q, Y, \psi, \varphi>$ как автомат $M_\beta \circ M = <X, Q_\beta \times Q, Y, \psi^\circ, \varphi^\circ>$, в котором для любого состояния $(s, q) \in Q_\beta \times Q$ и любого входного символа $x \in X$

$$\varphi^\circ(x, (s, q)) = \varphi(\varphi_\beta(x, s), q),\ \psi^\circ(x, (s, q)) = (\psi_\beta(\varphi^\circ(x, (s, q)), s), \psi(\varphi_\beta(x, s), q)).$$

Теорема 21. Пусть $f \in \Im^\tau_{l,l}(F)$ и автомат $M' = <X, Q', X, \psi', \varphi'>$ обратен к M_f с задержкой τ. Тогда справедливы следующие утверждения:

1. $f - z^{1+\tau}g \in \Im^{\tau}_{l,l}(F)$ для любого $g \in \Im_{l,l}(F)$ и $\tau(f - z^{1+\tau}g) = \tau(f)$.

2. Автомат $M_{t_0,z^{\tau+1}g} \circ M'$ обратен к $f - z^{1+\tau}g$ с задержкой τ. Для любого состояния q автомата $f - z^{1+\tau}g$ если (q, q') является τ-парой в $M_f \times M'$, то $(q, (q, q'))$ является τ-парой в $M_{f-z^{1+\tau}g} \times (M_{t_0,z^{\tau+1}g} \circ M')$, где, естественно, q рассматривается и как состояние в $M_{x_0,z^{\tau+1}g}$, и как состояние в M_f.

7.8. Общая схема FAPKC

Опишем общую схему FAPKC, в основном следуя [20]. По этой схеме произвольная криптосистема FPKC строится так.

Выбираются случайно такие два автомата f_1 и f_2 в $\Im'_{l,l}(F)$, для которых можно легко (за полиномиальное время) построить обратные к ним с некоторыми задержками τ_1 и τ_2 автоматы M'_1 и M'_2 соответственно. Строится $f = f_1 f_2$ по определению. Выбирается также некоторый автомат $g \in \Im_{l,l}(F)$. Пусть h_i есть память автомата f_i для $i = 1, 2$; $h = h_1 + h_2$; $\tau = \tau_1 + \tau_2$; $k = \mu(zg)$; M' является автоматом, обратным с задержкой τ к автомату M_f. По теореме 18 $M' = M'_2 \times M'^{(\tau_2)}_1$. Выбираются пары (q, r) и (s, r_1) в $X^h \times X^k$ для $X = F^l$. В них $q, s \in Q_f$. Применяя теоремы 20, 19, 17, 18 и 12, строятся τ-пары (q, q') и (s', s) в $M_f \times M'$ и $M' \times M_f$ соответственно, и s записывается как $s = \varepsilon\sigma$, где $\varepsilon \in X^{\tau}$, $\sigma \in X^{h-\tau}$.

Ключи и криптоалгоритмы в FAPKC определяются следующим образом.

Открытый ключ: $f, g, q, r, r_1, \sigma, \tau$.

Закрытый ключ: M', q', s'.

Шифрование: для заданного открытого текста $\alpha \in X^n$ выбирается случайно $\xi \in X^{\tau}$ и вычисляется шифртекст $\beta = \bar{\varphi}_{f+g}(\alpha\xi, qr) \in X^{n+\tau}$.

Расшифрование: открытый текст $\alpha \in X^n$ находится из $\zeta\alpha = \bar{\varphi}'(\bar{\varphi}_{1-zg}(\beta, r), q') \in X^{\tau+n}$ отбрасыванием несущественного слова $\zeta \in X^{\tau}$.

Подписание: подписью под сообщением $\alpha \in X^n$ является слово $\zeta\gamma = \bar{\varphi}'(\bar{\varphi}_{1-zg}(\alpha\xi, r_1), s') \in X^{\tau+n}$ для случайно выбранного $\xi \in X^{\tau}$; в ней $\zeta \in X^{\tau}$, $\gamma \in X^n$.

Проверка подписи: проверяющий принимает подпись $\zeta\gamma$, если $\delta = \alpha$ для $\delta = \bar{\varphi}_{f+zg}(\gamma, (\sigma\zeta, r_1))$, и отвергает её в противном случае.

Заметим, что если $g = 0$, $r = r_1 = \Lambda$ — пустое слово, то шифрование, расшифрование, подписание и проверка подписи в FAPKC сводятся к вычислениям

$$\beta = \bar{\varphi}_f(\alpha\xi, q);\ \zeta\alpha = \bar{\varphi}'(\beta, q');\ \zeta\gamma = \bar{\varphi}'(\alpha\xi, s');\ \delta = \bar{\varphi}_f(\gamma, \sigma\zeta) \tag{5}$$

соответственно. Иначе говоря, в этом случае шифрование состоит в преобразовании автоматом M_f в состоянии q открытого текста, дополненного суффиксом длиной τ, а расшифрование — в преобразовании шифртекста автоматом M' в соответствующем состоянии q' и удалении из результата преобразования префикса длиной τ; подписание состоит в преобразовании автоматом M' в состоянии s' подписываемого сообщения, дополненного суффиксом длиной τ, а проверка подписи под сообщением длиной n — в сравнении с ним результата преобразования суффикса подписи длиной n автоматом M_f в состоянии, составленном из суффикса соответствующего состояния s длиной $h - \tau$ и префикса подписи длиной τ.

Назовём известные на данный момент частные случаи, или версии, общей схемы FAPKC, получаемые при различных ограничениях на выбор её параметров. В них $F = GF(2)$.

1. *FAPKC* 0 [22], *FAPKC* 1,2 [23]: автомат f_2 линейный, $\tau(f_1) = 0$.

2. Tao R. J., 1992, цитируется по [20]: автомат f_2 линейный, $\tau(f_1) > 0$, у M_{f_1} имеется обратный с задержкой автомат вида $M_{A,zu}$ с $A \in M_{ll}(F[z])$ и $u \in \Im_{l,l}(F)$,

$l = 8$ и функция f выражается как $f(x_h, \ldots, x_1, x_0) = CT$, где $C \in M_{8,16}(F[z])$ и $T = (x_{0,1}, x_{0,2}, \ldots, x_{0,8}, x_{0,1}x_{-1,1}, x_{0,2}x_{-1,2}, \ldots, x_{0,8}x_{-1,8})^t$.

3. *FAPKC* 3 [24]: автомат f_2 линейный, $l = 8$, $f = CT$, $\mu(T) = 2$, $\tau_1 = 8$, $\tau_2 = 7$, $h_1 + h_2 \leqslant 20$.

4. [25]: $f_2 = B_2P_2Q_2$, $f_1 = B_1P_1Q_1$ или $f_1 = B_1$, где $B_i \in M_{l,l}(F[z])$, $Q_i \in M_{l,l}(F)$, каждое P_i есть биекция на X вида $x^{2^a+2^b}$.

В случае нелинейной выходной компоненты f_2 булево выражение композиции f_1f_2 может иметь непомерно большие размеры, даже если $\deg f_2 = 2$. Для того чтобы удержать размер открытого ключа в приемлемых границах, необходимо, чтобы параметры криптосистемы были очень маленькими, что видно из следующей таблицы [25], где для некоторых значений параметров l, h_1, h_2 демонстрируются соответствующие размеры в битах N_1 и N_2 открытого ключа в FAPKC с $\tau_2 \leqslant h_2 = \mu(f_2)$, $\tau_1 \leqslant h_1 = \mu(f_1)$ и соответственно с линейной и нелинейной функцией f_1.

l	7	7	5	5	3	3	3
(h_2, h_1)	(1,14)	(7,8)	(1,19)	(10,10)	(1,34)	(10,25)	(17,18)
N_1	8281	32948	4075	20950	1593	8883	13041
N_2	105840	414512	29850	181725	5400	34560	51192

7.9. Пример FAPKC

Рассмотрим «игрушечную» FAPKC, построенную по общей схеме со следующими конкретными значениями параметров в ней: $l = 1$, $F = GF(2)$, $g = 0$, $k = 0$, $r = r_1 = \Lambda$ — пустое слово. Таким образом, операции рассматриваемой криптосистемы выполняются по формулам (5).

Пусть, кроме того, автомат f_2 линейный с характеристиками $h_2 = 2$, $\tau_2 = 1$ и входо-выходными уравнениями

$$z_t = y_{t-2} + y_{t-1},\ t \geqslant 0; \tag{6}$$

автомат f_1 нелинейный с характеристиками $h_1 = 2$, $\tau_1 = 0$ и входо-выходными уравнениями

$$y_t = x_t + x_{t-1} + x_{t-2}x_{t-1},\ t \geqslant 0. \tag{7}$$

Подставляя (7) в (6), получим входо-выходные уравнения для $f = f_1f_2$:

$$z_t = x_{t-1} + x_{t-3} + x_{t-4}x_{t-3} + x_{t-3}x_{t-2},\ t \geqslant 0. \tag{8}$$

Таким образом, $h = 4$, $\tau = 1$; $M_{f_i} = <\{0,1\}, \{0,1\}^2, \{0,1\}, \psi_i, \varphi_i>$, $i = 1, 2$; $M_f = <\{0,1\}, \{0,1\}^4, \{0,1\}, \psi_f, \varphi_f>$ и функции переходов и выходов этих автоматов заданы следующими таблицами:

ψ_1

	$x_{-2}x_{-1}$			
x_0	00	01	10	11
0	00	10	00	10
1	01	11	01	11

φ_1

	$x_{-2}x_{-1}$			
x_0	00	01	10	11
0	0	1	0	0
1	1	0	1	1

ψ_2

	$y_{-2}y_{-1}$			
y_0	00	01	10	11
0	00	10	00	10
1	01	11	01	11

φ_2

	$y_{-2}y_{-1}$			
y_0	00	01	10	11
0	0	1	1	0
1	0	1	1	0

ψ_f

	$x_{-4}x_{-3}x_{-2}x_{-1}$							
x_0	0000	0001	0010	0011	0100	0101	0110	0111
0	0000	0010	0100	0110	1000	1010	1100	1110
1	0001	0011	0101	0111	1001	1011	1101	1111

ψ_f, продолжение

	$x_{-4}x_{-3}x_{-2}x_{-1}$							
x_0	1000	1001	1010	1011	1100	1101	1110	1111
0	0000	0010	0100	0110	1000	1010	1100	1110
1	0001	0011	0101	0111	1001	1011	1101	1111

φ_f

	$x_{-4}x_{-3}x_{-2}x_{-1}$							
x_0	0000	0001	0010	0011	0100	0101	0110	0111
0	0	1	0	1	1	0	0	1
1	0	1	0	1	1	0	0	1

φ_f, продолжение

	$x_{-4}x_{-3}x_{-2}x_{-1}$							
x_0	1000	1001	1010	1011	1100	1101	1110	1111
0	0	1	0	1	0	1	1	0
1	0	1	0	1	0	1	1	0

Видно, что функция φ_1 биективна в каждом состоянии, поэтому автомат f_1 действительно обратим с задержкой $\tau_1 = 0$ (см., например, теорему 20). В обратном к нему с задержкой 0 автомате $M_1' = <\{0,1\}, \{0,1\}^2, \{0,1\}, \psi_1', \varphi_1'>$ функции ψ_1', φ_1' получаются по правилу: если $\psi_1(x,q) = s$ и $\varphi_1(x,q) = y$, то $\psi_1'(y,q) = s$ и $\varphi_1'(y,q) = x$. Полученные так, они показаны в следующих таблицах:

ψ_1'

	$x_{-2}x_{-1}$			
y_0	00	01	10	11
0	00	11	00	10
1	01	10	01	11

φ_1'

	$x_{-2}x_{-1}$			
y_0	00	01	10	11
0	0	1	0	0
1	1	0	1	1

Входо-выходные уравнения для автомата M_1' получаются непосредственно из (7):

$$x_t = y_t + x_{t-1} + x_{t-2}x_{t-1},\ t \geqslant 0. \tag{9}$$

Для обращения с задержкой $\tau_2 = 1$ автомата f_2 воспользуемся теоремой 19. В самом деле, для автомата f_2 справедливо $f_2(x_{-2}x_{-1}x_0) = x_{-2} + x_{-1}$, поэтому f_2 задаётся матрицей $B =\| z^2 + z \| \in M_{1,1}(F[z])$, представимой как $B = PDQ(1 + zA)$ для $P = =\| 1 \| \in GL_1(F[z])$, $Q =\| 1 \| \in GL_1(F)$, $D =\| z \| \in M_{1,1}(F[z])$, $A =\| 1 \| \in M_{1,1}(F[z])$. Положив, $C = z^{\tau_2}D^{-1}$ и $B' = Q^{-1}CP^{-1}$, будем иметь $C =\| 1 \|$ и $B' =\| 1 \|$. Тогда по теореме 19 автомат M_2', задаваемый матрицей $B' + zA =\| 1 + z \|$, является обратным с задержкой $\tau_2 = 1$ к автомату f_2 и (00,0) есть τ_2-пара в $M_{f_2} \times M_2'$. Входо-выходная функция автомата M_2' есть $f_2'(z_{-1}z_0) = z_{-1} + z_0$, поэтому $M_2' = <\{0,1\}, \{0,1\}, \{0,1\}, \psi_2', \varphi_2'>$ и таблицы функций ψ_2', φ_2' следующие:

ψ_2'

	z_{-1}	
z_0	0	1
0	0	1
1	1	0

φ_2'

	z_{-1}	
z_0	0	1
0	0	1
1	1	0

В автомате $M_1'^{(\tau_2)} = <\{0,1\}, \{0,1\}^2 \times \{0,1,\ldots,\tau_2\}, \{0,1\}, \psi_1'^{(\tau_2)}, \varphi'^{(\tau_2)})_1>$ функции $\psi_1'^{(\tau_2)}$, $\varphi_1'^{(\tau_2)}$ задаются таблицами

$\psi_1'^{\tau_2}$

	$y_{-2}y_{-1}i$							
y_0	000	010	100	110	001	011	101	111
0	001	011	101	111	001	111	001	101
1	001	011	101	111	011	101	011	111

$\varphi_1'^{\tau_2}$

	$y_{-2}y_{-1}i$							
y_0	000	010	100	110	001	011	101	111
0	0	0	0	0	0	1	0	0
1	0	0	0	0	1	0	1	1

Наконец, автомат $M' = M_2' \times M_1'^{(\tau_2)} = <\{0,1\}, \{0,1\} \times (\{0,1\}^2 \times \{0,1,\ldots,\tau_2\}), \{0,1\}, \psi', \varphi'>$ задаётся таблицами переходов и выходов

ψ'

	$z_{-1}y_{-2}y_{-1}i$							
z_0	0000	0010	0100	0110	0001	0011	0101	0111
0	0001	0011	0101	0111	0001	0111	0001	0101
1	1001	1011	1101	1111	1011	1101	1011	1111

ψ', продолжение

	$z_{-1}y_{-2}y_{-1}i$							
z_0	1000	1010	1100	1110	1001	1011	1101	1111
0	1001	1011	1101	1111	1011	1101	1011	1111
1	0001	0011	0101	0111	0001	0111	0001	0101

φ'

	$z_{-1}y_{-2}y_{-1}i$							
z_0	0000	0010	0100	0110	0001	0011	0101	0111
0	0	0	0	0	0	1	0	0
1	0	0	0	0	1	0	1	1

φ', продолжение

	$z_{-1}y_{-2}y_{-1}i$							
z_0	1000	1010	1100	1110	1001	1011	1101	1111
0	0	0	0	0	1	0	1	1
1	0	0	0	0	0	1	0	0

Пусть $q = 0111 \in Q_f$. Пользуясь теоремой 10, найдём $(q_1, q_2) \in Q_{f_1} \times Q_{f_2}$: $q_1 = 11$, $q_2 = \bar{\varphi}_1(11, 01) = 01$. По теореме 20 $(q_1, q_1') = (q_1, q_1) = (11, 11)$ является 0-парой в $M_{f_1} \times M_1'$. Имея τ_2-пару $(s_2, s_2') = (00, 0)$ в $M_{f_2} \times M_2'$, вычислим $q_2' = \psi_2'(\bar{\varphi}_2(q_2, s_2), s_2') = = \psi_2'(\bar{\varphi}_2(01, 00), 0) = \psi_2'(00, 0) = 0$. По теореме 17 $(q_2, q_2') = (01, 0)$ является τ_2-парой в $M_{f_2} \times M_2'$, и по теореме 18 $(q, q') = (q, (q_2', (q_1', 0)) = (0111, 0110)$ является τ-парой в $M_f \times M'$.

Непосредственно проверяется, что последовательность

$$\alpha 1 = 0100100001100101011011000110110001101111$$

автомат M_f в состоянии $q = 0111$ зашифровывает в последовательность

$$\beta = 1110110100110010000101100011011000110111,$$

которую автомат M' в состоянии $q' = 0110$ расшифровывает в последовательность 0α.

Помня о недопустимости применения в разных приложениях криптографических ключей, легко вычислимых один из другого, выберем τ-пару (s', s) в $M' \times M_f$ независимо от выбранной τ-пары (q, q') в $M_f \times M'$. Для этого, аналогично (q, q'), построим ещё одну τ-пару в $M_f \times M'$ — скажем, $(u, u') = (1101, 0010)$, и по ней, пользуясь теоремой 12, построим τ-пару (s', s) в $M' \times M_f$, положив $s = u = 1101$ и $s' = \psi'(\bar{\varphi}(\xi, u), u') = \psi'(\bar{\varphi}(0, 1101), 0010) = \psi'(1, 0010) = 1011$. Представив s как $s = \beta\sigma$ для $\beta \in X^\tau$, будем иметь $\sigma = 101$.

Непосредственно проверяется, что последовательность $\alpha 1$ автомат M' в состоянии $s' = 1011$ преобразует в слово

$$\zeta\gamma = 0\gamma = 0000101011111001001001010010010100100111,$$

которое принимается за подпись под сообщением α. Для проверки подлинности этой подписи убеждаемся, что автомат M_f в состоянии $\sigma\zeta = 1010$ действительно преобразует слово γ в сообщение α.

ЛИТЕРАТУРА

1. *Агибалов Г. П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского госуниверситета. Приложение. 2003. № 6. С. 31–41.
2. *Агибалов Г. П.* Логические уравнения в криптоанализе сжимающего и самосжимающего генераторов // Вестник Томского госуниверситета. Приложение. 2004. № 9(I). С. 49–54.
3. *Фомичёв В. М.* Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003. 400 с.
4. *Бабаш А. В., Шанкин Г. П.* Криптография. М.: Солон-Р, 2002. 512 с.

5. *Агибалов Г. П., Оранов А. М.* Лекции по теории конечных автоматов. Томск: Изд-во Том. ун-та, 1984. 185 с.
6. *Menezes A., van Oorshot P., Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1996. 661 pp.
7. *Watanabe D., Furuya S., Yoshida H., Takaragi K., Preneel B.* A New Keystream Generator MUGI // LNCS. 2002. No. 2365. P. 179–194.
8. *Joux A., Muller F.* Loosening the KNOT // LNCS. 2003. No. 2887. P. 87–99.
9. *Golic J. Dj., Bagini V., Morgari G.* Linear Cryptanalysis of Bluetooth Stream Cipher // LNCS. 2002. No. 2332. P. 238–255.
10. *O'Neil S., Gittins B., Landman H.* VEST. Hardware-Dedicated Stream Cipher // eSTREAM. October 2005. 63 p.
11. *Wolfram S.* Cryptography with Cellular Automata // LNCS. 1985. No. 218. P. 429–432.
12. *Michaljevic' M., Zheng Y., Imai H.* A Cellular Automaton Based Fast One-Way Hash Function Suitable for Hardware Implementation // LNCS. 1998. No. 1431. P. 217–233.
13. *Шеннон К. Э.* Математическая теория связи // Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 243–332.
14. *Stamp M. Low R. M.* Applied Cryptanalysis. Breaking Ciphers in the Real World. NJ: John Wiley & Sons, 2007. 400 p.
15. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.
16. *Мур Э. Ф.* Умозрительные эксперименты с последовательностными машинами // Автоматы / сб. статей под ред. К. Э. Шеннона и Дж. Маккарти. М.: ИЛ, 1956. С. 179–210.
17. *Панкратов И. В.* К определению понятия самосинхронизирующегося поточного шифра // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 114–117.
18. *Панкратов И. В.* О поточных и автоматных шифрсистемах // Прикладная дискретная математика. Приложение. 2009. № 1. С. 21–24.
19. *Панкратов И. В.* О поточных и автоматных шифрсистемах с симметричным ключом // Прикладная дискретная математика. 2009. № 3. С. 59–68.
20. *Dai Z. D., Ye D. F., Lam K. Y.* Weak Invertability of Finite Automata and Cryptanalysis on FAPKC // LNCS. 1998. No. 1514. P. 227–241.
21. *Tao R. J.* On Invertability of Some Compound Finite Automata // Laboratory for Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 10080, China, ISCAS–LCS–95–06.
22. *Tao R. J., Chen S. H.* A Finite Automaton Public Key Cryptosystem and Digital Signatures // Chinese J. of Comptuter. 1985. V. 8. P. 401–409 (in Chinese).
23. *Tao R. J., Chen S. H.* Two Varieties of Finite Automaton Public Key Cryptosystem and Digital Signatures // J. of Compt. Sci. and Tech. 1986. V. 1. No. 1. P. 9–18.
24. *Tao R. J., Chen S. H., Chen X. M.* FPKC3: a New Finite Automaton Public Key Cryptosystem // Laboratory for Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 10080, China, June 1995. ISCAS–LCS–95–07.
25. *Chen X. M.* The Invertability Theory and Application of Quadratic Finite Automata // Laboratory for Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 10080, China, 1996. Doctoral Thesis.