2008 Математические методы криптографии № 2(2)
DOI 10.17223/20710410/2/8

УДК 681.3

ПРЕДСТАВЛЕНИЕ КРИПТОСИСТЕМ МНОГООСНОВНОЙ АЛГЕБРАИЧЕСКОЙ СИСТЕМОЙ

Е.А. Иващенко, В.Г. Скобелев

Донецкий национальный университет,
Институт прикладной математики и механики НАН Украины, *г. Донецк*

E-mail: eugenia1000@rambler.ru, skbv@iamm.ac.donetsk.ua

На основе многоосновной алгебраической системы построена формальная модель криптосистемы. В рамках этой модели выделены основные типы криптосистем.

Ключевые слова: *модель криптосистемы*, *многоосновная алгебраическая система.*

Современные задачи криптографии обуславливают необходимость разработки математического аппарата для моделирования систем защиты информации, их сравнительной характеристики, анализа их вычислительной стойкости и имитостойкости. Системы защиты информации [1 – 3] характеризуются многообразием и сложностью процессов их взаимодействия с внешней средой, а также сложностью внешней среды (содержащей интеллектуальные компоненты). При этом математическая модель криптосистемы играет фундаментальную роль. Известны подходы к построению таких моделей с позиций теории систем [4] и современной алгебры [5].

Первый подход [1] базируется на системе вход-выходного типа

$$S = (M , C , K_1 , K_2 , E , D) ,$$

где M, C, K_1 и K_2 – множество соответственно открытых текстов, шифртекстов, ключей шифрования и ключей расшифровки, а $E : M \times K_1 \to C$ и $D : C \times K_2 \to M$ – алгоритмы шифрования и расшифровки. Достоинство этой модели – представление согласованности процессов шифрования и расшифровки биекцией $k : K_1 \to K_2$, возможность выделения блочных и поточных криптосистем, а также ряда портов, через которые осуществляются пассивные атаки криптоаналитика.

Второй подход [6] основан на алгебраической системе

$$S = (T , F, domain , range , F_e , F_c) ,$$

где T и F – множество имен соответственно типов и функций, $domain : F \to T^*$ и $range : F \to T$ – отображения, F_e ($F_e \subseteq F$) – множество легко вычислимых функций, а $F_c = \{ f \in F \mid domain (f) = \lambda \}$ (λ – пустое слово) – множество констант. Достоинство этой модели – возможность построения на множестве термов системы конгруэнций, предназначенной для формирования определяющих соотношений для конкретной криптосистемы, и выделения ряда портов, через которые осуществляются пассивные атаки криптоаналитика.

Однако обе модели имеют существенные недостатки. Во-первых, они могут представлять системы с предвосхищением и системы, содержащие невычислимые функции. Во-вторых, необходима их дополнительная проработка для выделения основных классов криптосистем [1] и представления основных типов атак криптоаналитика. В-третьих, они не дают возможность эффективно представлять параметрические криптосистемы [7, 8], нестационарные криптосистемы и криптосистемы с вариацией окна шифрования. Естественный путь устранения этих недостатков – это выбор в качестве базовой модели варианта системы алгоритмических алгебр [9]. Для этого необходимо построить соответствующую многоосновную алгебраическую систему. Решение этой задачи – основная цель настоящей работы.

Структура работы следующая: в п.1 построена и охарактеризована базовая многоосновная алгебраическая система, в п.2 в рамках этой модели выделены основные типы криптосистем. Заключение содержит ряд выводов.

1. Базовая алгебраическая система

Рассмотрим многоосновную алгебраическую систему

$$\mathsf{S} = (\mathsf{T} , \mathsf{F}),$$

где семейство T основных множеств и сигнатура F имеют вид

$$\mathsf{T} = \{ T_{ij} = \{ t_{ij}^{(r)} \mid r \in \mathbf{N} \} \mid i = 1, \ldots, 8 ; j = 1, 2 \},$$

$$\mathsf{F} = U \cup F \cup K \cup \Phi .$$

Предполагается, что множества T_{ij} попарно не пересекаются, причем T_{i2} ($i = 1, \ldots, 8$) так линейно упорядочены, что

$$t_{i2}^{(1)} < t_{i2}^{(2)} < \ldots < t_{i2}^{(n)} < \ldots$$

Множества $T_{11}, \ldots, T_{81}$ и $T_{12}, \ldots, T_{82}$ назовем множествами имен и множествами размеров соответственно открытых текстов, ключей шифрования, параметров шифрования, состояний шифрования, шифртекстов, ключей расшифровки, параметров расшифровки и состояний расшифровки.

Охарактеризуем теперь сигнатуру F, состоящую из имен легко вычислимых функций.

I. Множество U состоит из имен монотонно возрастающих функций и имеет вид

$$U = \{ u_i^{(1)} : \mathbf{N} \to \mathbf{N},\ u_i^{(2)} : \mathbf{N}^3 \to \mathbf{N},\ u_i^{(3)} : \mathbf{N}^3 \to \mathbf{N} \mid i = 1, \ldots, 8 \},$$

где для всех значений $i \in \{ 1, \ldots, 8 \}$ при любых фиксированных значениях $y, z \in \mathbf{N}$ ($z < y$) функция $v_i(x) = u_i^{(2)}(x, y, z)$ − кусочно-постоянная, а функция $w_i(x) = u_i^{(3)}(x, y, z)$ − периодическая на множестве $\{ 1, \ldots, u_i^{(1)}(y) \}$, и каждая из функций v_i, w_i отображает это множество на множество $\{ 1, \ldots, u_i^{(1)}(z) \}$.

Множество U предназначено для построения на каждом множестве $T_{i1}T_{i2}$ ($i = 1, \ldots, 8$) системы определяющих соотношений вида

$$\begin{cases} t_{i1}^{(h)} t_{i2}^{(r)} = t_{i1}^{(h - u_i^{(1)}(r))} t_{i2}^{(r)}, & \text{если } h > u_i^{(1)}(r), \\ t_{i1}^{(h)} t_{i2}^{(r)} = t_{i1}^{(h_1)} t_{i2}^{(r_1)} t_{i1}^{(h_2)} t_{i2}^{(r_2)}, \end{cases} \tag{1}$$

где

$$r = r_1 + r_2 \ (r_1, r_2) \in \mathbf{N},$$

$$h_1 = u_i^{(2)}(h, r, r_1),$$

$$h_2 = u_i^{(3)}(h, r, r_2).$$

Первое из соотношений (1) осуществляет переход от множества $T_{i1}T_{i2}$ ($i = 1, \ldots, 8$) к множеству

$$T_{i,12} = \{ t_{i1}^{(h)} t_{i2}^{(r)} \mid r \in \mathbf{N},\ h \in \{ 1, \ldots, u_i^{(1)}(r) \} \} \subset T_{i1}T_{i2}.$$

Положим

$$T_{i,12}(n) = \{ t_{i1}^{(h)} t_{i2}^{(n)} \in T_{i,12} \mid h \in \{ 1, \ldots, u_i^{(1)}(n) \} \} \ (n \in \mathbf{N}).$$

Тогда

$$T_{i,12} = \bigcup_{n=1}^{\infty} T_{i,12}(n),$$

где $T_{i,12}(n)$ ($n \in \mathbf{N}$) – попарно непересекающиеся конечные множества. Значение второго из соотношений (1) состоит в следующем. Систему соотношений (1) назовем полугрупповой, если каждый элемент $t_{i1}^{(h)} t_{i2}^{(r)} \in T_{i,12}$ ($i = 1, \ldots, 8$) единственным образом представляется в виде

$$t_{i1}^{(h)} t_{i2}^{(r)} = t_{i1}^{(h_1)} t_{i2}^{(1)} \ldots t_{i1}^{(h_r)} t_{i2}^{(1)}.$$

Пусть $X = \{ x_1, \ldots, x_m \}$ ($m \in \mathbf{N}$), $t_{i2}^{(r)} = r$ ($r \in \mathbf{N}$) и $u_i^{(1)}(r) = m^r$. Определим биекцию $\varphi : T_{i,12} \to X^+$ равенствами

$$\varphi(t_{i1}^{(h)} t_{i2}^{(r)}) = x_{j_1} \ldots x_{j_r} \quad (h = 1, \ldots, u_i^{(1)}(r)) \ (r \in \mathbf{N}),$$

где

$$h = j_r + (j_{r-1} - 1)\, m + (j_{r-2} - 1)\, m^2 + \ldots + (j_1 - 1)\, m^{r-1}.$$

В этом случае соотношения (1) согласуются с лексикографическим порядком на каждом множестве $T_{i,12}(r)$ ($r \in \mathbf{N}$). Отсюда вытекает

Теорема 1. Полугрупповая система определяющих соотношений (1) непротиворечива.

Проиллюстрируем достоинства полугрупповой системы определяющих соотношений (1) на следующем простом примере.

Пример 1. 1. Пусть

$$X = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

Первое соотношение (1) дает возможность представить сообщение $t_{11}^{(22)} t_{12}^{(1)}$ в виде

$$t_{11}^{(20)} t_{12}^{(1)} = t_{11}^{(12)} t_{12}^{(1)} = t_{11}^{(4)} t_{12}^{(1)} = 011.$$

2. Пусть

$$X = \mathbf{Z}_4 = \{000, 001, 010, 011\}.$$

Второе соотношение (1) дает возможность представить сообщение $t_{11}^{(21)}t_{12}^{(2)}$ в виде

$$t_{11}^{(21)}t_{12}^{(2)} = t_{11}^{(5)}t_{12}^{(2)} = t_{11}^{(2)}t_{12}^{(1)}t_{11}^{(4)}t_{12}^{(1)} = 001000 .$$

Всюду в дальнейшем считаем, что система определяющих соотношений (1) – полугрупповая и истинны равенства

$$u_i^{(1)} = u_{i+4}^{(1)} \quad (i = 1, \ldots, 4) .$$

II. Множество F имеет вид

$$F = F_1 \cup F_2 ,$$

где F_1 и F_2 – равномощные непересекающиеся множества имен функций, удовлетворяющие следующим трем условиям.

Условие 1. Для каждого $f_j \in F_j$ $(j = 1, 2)$ существуют такие числа $n_{f_j}^{(1)}$, $n_{f_j}^{(2)} \in \mathbf{N}$, что

$$\mathrm{Dom}\, f_j = (\bigcup_{n=1}^{\infty} (T_{4j-3,12}(n) \times T_{4j-2,12}(n))) \times T_{f_j} ,$$

$$\mathrm{Val}\, f_j = \bigcup_{n=1}^{\infty} T_{9-4j,12}(n),$$

где $$\varnothing \neq T_{f_j} \subseteq T_{4j-1,12}(n_{f_j}^{(1)}) \times T_{4j,12}(n_{f_j}^{(2)}) .$$

Условие 2. Для всех $f_j \in F_j$ $(j = 1, 2)$ и $(t_{4j-3}, t_{4j-2}) \in T_{4j-3,12}(n) \times T_{4j-2,12}(n)$ $(n \in \mathbf{N})$,

$$f_j(t_{4j-3}, t_{4j-2}, t_{4j-1}, t_{4j}) \in T_{9-4j,12}(n)$$

при всех $(t_{4j-1}, t_{4j}) \in T_{f_j}$.

Условие 3. Для всех $f_j \in F_j$ $(j = 1, 2)$ функция

$$g_{f_j, t_{4j-2}, t_{4j-1}, t_{4j}}(t_{4j-3}) = f_j(t_{4j-3}, t_{4j-2}, t_{4j-1}, t_{4j,12})$$

является биекцией множества $T_{4j-3,12}(n)$ $(n \in \mathbf{N})$ на множество $T_{9-4j,12}(n)$ при всех фиксированных значениях $(t_{4j-2}, t_{4j-1}, t_{4j}) \in T_{4j-2,12}(n) \times T_{f_j}$.

Назовем F_1 множеством схем шифрования, а F_2 – множеством схем расшифровки.

III. Множество

$$K = \{\kappa_1, \kappa_2\}$$

состоит из имен таких биекций

$$\kappa_j : F_j \to F_{3-j} \quad (j = 1, 2) ,$$

что для всех $f_j \in F_j$ $(j = 1, 2)$ истинны равенства

$$|pr_1 T_{f_j}| = |pr_1 T_{\kappa_j(f_j)}| ,$$

$$|pr_2 T_{f_j}| = |pr_2 T_{\kappa_j(f_j)}| ,$$

$$|T_{f_j}| = |T_{\kappa_j(f_j)}| ,$$

IV. Множество

$$\Phi = \bigcup_{j=1}^{2} \bigcup_{f_j \in F_j} \{\alpha_{f_j,n}, \beta_{f_j}, \gamma_{f_j} \mid n \in \mathbf{N}\}$$

состоит из имен таких биекций

$$\alpha_{f_j,n} : T_{4j-2,12}(n) \to T_{(4j+2)(\mathrm{mod}\ 8),12}(n) ,$$

$$\beta_{f_j} : pr_1 T_{f_j} \to pr_1 T_{\kappa_j(f_j)} ,$$

$$\gamma_{f_j} : pr_2 T_{f_j} \to pr_2 T_{\kappa_j(f_j)} ,$$

что для всех $f_j \in F_j$ $(j = 1, 2)$ и $n \in \mathbf{N}$ равенства

$$\kappa_j(f_j)(f_j(t_{4j-3}, t_{4j-2}, t_{4j-1}, t_{4j}), \alpha_{f_j,n}(t_{4j-2}), \beta_{f_j}(t_{4j-1}), \gamma_{f_j}(t_{4j})) = t_{4j-3} \qquad (2)$$

истинны при всех $(t_{4j-3}, t_{4j-2}, t_{4j-1}, t_{4j}) \in T_{4j-3,12}(n) \times T_{4j-2,12}(n) \times T_{f_j}$.

Отметим, что равенства (2) обеспечивают взаимно-однозначное соответствие между результатами процессов шифрования и расшифровки.

Охарактеризуем теперь построенную алгебраическую систему S.

Для всех $f_j \in F_j$ $(j = 1, 2)$ и $n \in \mathbf{N}$ определим отношения эквивалентности

$$\varepsilon_1(f_j, n) \subseteq T_{4j-2,12}(n) \times T_{4j-2,12}(n),$$

$$\varepsilon_2(f_j) \subseteq pr_1 T_{f_j} \times pr_1 T_{f_j},$$

$$\varepsilon_3(f_j) \subseteq pr_2 T_{f_j} \times pr_2 T_{f_j}$$

следующим образом:

$$(t_{4j-2}, t'_{4j-2}) \in \varepsilon_1(f_j, n) \Leftrightarrow$$

$$\Leftrightarrow (\forall (t_{4j-3}, t_{4j-1}, t_{4j}) \in T_{4j-3,12}(n) \times T_{f_j})(f_j(t_{4j-3}, t_{4j-2}, t_{4j-1}, t_{4j}) =$$

$$= f_j(t_{4j-3}, t'_{4j-2}, t_{4j-1}, t_{4j})); \tag{3}$$

$$(t_{4j-1}, t'_{4j-1}) \in \varepsilon_2(f_j) \Leftrightarrow$$

$$\Leftrightarrow (\forall n \in \mathbf{N})(\forall (t_{4j-3}, t_{4j-2}, t_{4j}) \in T_{4j-3,12}(n) \times T_{4j-3,12}(n) \times \mathrm{pr}_2 T_{f_j})(f_j(t_{4j-3}, t_{4j-2}, t_{4j-1}, t_{4j}) =$$

$$= f_j(t_{4j-3}, t_{4j-2}, t'_{4j-1}, t_{4j})); \tag{4}$$

$$(t_{4j}, t'_{4j}) \in \varepsilon_2(f_j) \Leftrightarrow$$

$$\Leftrightarrow (\forall n \in \mathbf{N})(\forall (t_{4j-3}, t_{4j-2}, t_{4j-1}) \in T_{4j-3,12}(n) \times T_{4j-2,12}(n) \times \mathrm{pr}_1 T_{f_j})(f_j(t_{4j-3}, t_{4j-2}, t_{4j-1}, t_{4j}) =$$

$$= f_j(t_{4j-3}, t_{4j-2}, t_{4j-1}, t'_{4j})). \tag{5}$$

Из (2) – (5) вытекает

Теорема 2. Для всех $f_j \in F_j$ $(j = 1, 2)$:

1) если $(t_{4j-2}, t'_{4j-2}) \in \varepsilon_1(f_j, n)$ $(n \in \mathbf{N})$, то $(\alpha_{f_j,n}(t_{4j-2}), \alpha_{f_j,n}(t'_{4j-2})) \in \varepsilon_1(\kappa_j(f_j), n)$;

2) если $(t_{4j-1}, t'_{4j-1}) \in \varepsilon_2(f_j)$, то $(\beta_{f_j}(t_{4j-1}), \beta_{f_j}(t'_{4j-1})) \in \varepsilon_2(\kappa_j(f_j), n)$;

3) если $(t_{4j}, t'_{4j}) \in \varepsilon_3(f_j)$, то $(\gamma_{f_j}(t_{4j-1}), \gamma_{f_j}(t'_{4j-1})) \in \varepsilon_3(\kappa_j(f_j), n)$.

Отметим, что рассмотренные выше понятия дают возможность выделить следующие классы систем S:

1) класс слабо F-минимальных систем S, характеризующийся тем, что для любых двух элементов $f_j, f'_j \in F_j$ $(j = 1, 2)$ при любом $(t_{4j-1}, t_{4j}) \in T_{f_j} \cap T_{f'_j}$ существует такое число $n \in \mathbf{N}$ и такой элемент $t_{4j-2} \in T_{4j-2,12}(n)$, что

$$g_{f_j, t_{4j-2}, t_{4j-1}, t_{4j}} \neq g_{f'_j, t_{4j-2}, t_{4j-1}, t_{4j}};$$

2) класс сильно F-минимальных систем S, характеризующийся тем, что для любых двух элементов $f_j, f'_j \in F_j$ $(j = 1, 2)$

$$g_{f_j, t_{4j-2}, t_{4j-1}, t_{4j}} \neq g_{f'_j, t_{4j-2}, t_{4j-1}, t_{4j}}$$

при любом $(t_{4j-1}, t_{4j}) \in T_{f_j} \cap T_{f'_j}$ для всех $t_{4j-2} \in T_{4j-2,12}(n)$ $(n \in \mathbf{N})$;

3) класс K-минимальных систем S, характеризующихся тем, что

$$\kappa_1^{-1} = \kappa_2;$$

4) класс K-минимальных систем S, характеризующийся тем, что для всех $f_j \in F_j$ $(j = 1, 2)$ каждое отношение $\varepsilon_1(f_j, n)$ $(n \in \mathbf{N})$ – отношение равенства на множестве $T_{4j-2,12}(n)$.

2. Классы криптосистем

Для каждого $f_j \in F_j$ $(j = 1, 2)$ и $(t_{4j-1}, t_{4j}) \in T_{f_j}$ определим отображение

$$A_{f_j, t_{4j-1}, t_{4j}} : \bigcup_{n=1}^{\infty} (T_{4j-3,12}(n) \times T_{4j-2,12}(n)) \to \bigcup_{n=1}^{\infty} T_{9-4j,12}(n) \quad (j = 1, 2)$$

равенством $$A_{f_j, t_{4j-1}, t_{4j}}(t_{4j-3}, t_{4j-2}) = f_j(t_{4j-3}, t_{4j-2}, t_{4j-1}, t_{4j}).$$

Отображение A_{f_1, t_3, t_4} $(f_1 \in F_1, (t_3, t_4) \in T_{f_1})$ назовем алгоритмом (f_1, t_3, t_4)-шифрования, а отображение A_{f_2, t_7, t_8} $(f_2 \in F_2, (t_7, t_8) \in T_{f_2})$ – алгоритмом (f_2, t_7, t_8)-расшифровки.

Отметим, что такое определение алгоритмов шифрования и расшифровки дает возможность в терминах многоосновной алгебраической системы S выделить следующие три уровня понятия «ключ»:

1) элемент множества $T_{4j-2,12}$ интерпретируется как сеансовый или, иными словами, кратковременный ключ;

2) элемент множества $pr_2\, T_{f_j}$ интерпретируется как ключ средней длительности, т.е. как ключ, применяемый для определенного числа сеансов;

3) элемент множества $pr_1\, T_{f_j}$ интерпретируется как долговременный ключ.

Определим стационарную (f_1, t_3, t_4)-криптосистему $(f_1 \in F_1, (t_3, t_4) \in T_{f_1}))$ как упорядоченную пару

$$C_{f_1,t_3,t_4} = (A_{f_1,t_3,t_4}, A_{\kappa_1(f_1),\beta_{f_1}(t_3),\gamma_{f_1}(t_4)}),$$

а стационарную (f_2, t_7, t_8)-криптосистему $(f_2 \in F_2, (t_7, t_8) \in T_{f_2})$ – как упорядоченную пару

$$C_{f_2,t_7,t_8} = (A_{\kappa_2(f_2),\beta_{f_2}(t_7),\gamma_{f_2}(t_8)}, A_{f_2,t_7,t_8}).$$

Отметим, что определение криптосистемы как упорядоченной пары дает возможность выделить (если такая необходимость возникает), что является приоритетным: процесс шифрования или процесс расшифровки.

Покажем, что в терминах многоосновной алгебраической системы S могут быть представлены основные классы криптосистем.

Стационарную (f_j, t_{4j-1}, t_{4j})-криптосистему $C_{f_j,t_{4j-1},t_{4j}}$ $(f_j \in F_j\ (j = 1, 2), (t_{4j-1}, t_{4j}) \in T_{f_j})$ назовем:

1) симметричной криптосистемой, если каждое $\alpha_{f_j,n}$ $(n \in \mathbf{N})$ – имя такой биекции, что $\alpha^{-1}_{f_j,n}$ – имя легковычислимой биекции;

2) асимметричной, если каждое $\alpha_{f_j,n}$ $(n \in \mathbf{N})$ – имя такой биекции, что в настоящее время не известен быстрый алгоритм вычисления биекции $\alpha^{-1}_{f_j,n}$, либо доказано, что такой алгоритм не существует;

3) криптосистемой с автоключом, если $t_{4j-2} \in T_{4j-3,12}$ – фиктивная переменная;

4) криптосистемой с внешним сеансовым ключом, если $t_{4j-2} \in T_{4j-3,12}$ – существенная переменная;

5) параметрической криптосистемой, если $t_{4j-1} \in pr_1\, T_{f_j}$ – существенный параметр для системы $C_{f_j,t_{4j-1},t_{4j}}$, т.е. существуют два таких элемента $t_{4j-1}, t'_{4j-1} \in pr_1\, T_{f_j}$, что

$$C_{f_j,t_{4j-1},t_{4j}} \neq C_{f_j,t'_{4j-1},t_{4j}};$$

6) блочной криптосистемой, если

$$A_{f_j,t_{4j-1},t_{4j}}(t_{4j-3}t'_{4j-3}, t_{4j-2}t'_{4j-2}) = A_{f_j,t_{4j-1},t_{4j}}(t_{4j-3}, t_{4j-2})\, A_{f_j,t_{4j-1},t_{4j}}(t'_{4j-3}, t'_{4j-2})$$

для всех $(t_{4j-3}, t_{4j-2}), (t'_{4j-3}, t'_{4j-2}) \in \bigcup_{n=1}^{\infty} (T_{4j-3,12}(n) \times T_{4j-2,12}(n))$;

7) схемой с предысторией, если существует хотя бы одна такая пара значений

$$(t_{4j-3}, t_{4j-2}), (t'_{4j-3}, t'_{4j-2}) \in \bigcup_{n=1}^{\infty} (T_{4j-3,12}(n) \times T_{4j-2,12}(n)),$$

что $A_{f_j,t_{4j-1},t_{4j}}(t_{4j-3}t'_{4j-3}, t_{4j-2}t'_{4j-2}) \neq A_{f_j,t_{4j-1},t_{4j}}(t_{4j-3}, t_{4j-2})\, A_{f_j,t_{4j-1},t_{4j}}(t'_{4j-3}, t'_{4j-2})$.

Выделим следующий подкласс класса схем с предысторией, являющийся предметом исследования классической криптографии. Стационарную (f_j, t_{4j-1}, t_{4j})-криптосистему с предысторией $C_{f_j,t_{4j-1},t_{4j}}$ $(f_j \in F_j\ (j = 1, 2), (t_{4j-1}, t_{4j}) \in T_{f_j})$ назовем стационарной поточной криптосистемой, если существует такая легко вычислимая функция

$$\delta_{f_j,t_{4j-1},t_{4j}} : T_{f_j} \times \bigcup_{n=1}^{\infty} (T_{4j-3,12}(n) \times T_{4j-2,12}(n)) \to T_{f_j}, \tag{6}$$

что для всех $(t_{4j-3}, t_{4j-2}), (t'_{4j-3}, t'_{4j-2}) \in \bigcup_{n=1}^{\infty} (T_{4j-3,12}(n) \times T_{4j-2,12}(n))$

$$A_{f_j,t_{4j-1},t_{4j}}(t_{4j-3}t'_{4j-3}, t_{4j-2}t'_{4j-2}) = A_{f_j,t_{4j-1},t_{4j}}(t_{4j-3}, t_{4j-2})\, A_{f_j,t_{4j-1},t'_{4j}}(t'_{4j-3}, t'_{4j-2}), \tag{7}$$

где $$t'_{4j} = \delta_{f_j,t_{4j-1},t_{4j}}(t_{4j}, (t_{4j-3}, t_{4j-2})). \tag{8}$$

Из (1) вытекает следующая

Теорема 3. Для любой стационарной поточной криптосистемы $C_{f_j,t_{4j-1},t_{4j}}$ ($f_j \in F_j$ ($j = 1, 2$), (t_{4j-1}, t_{4j}) $\in T_{f_j}$) отображение $A_{f_j,t_{4j-1},t_{4j}}$ – ограниченно-детерминированная функция.

Следующий пример показывает, что современные криптосистемы естественно укладываются в рамки построенной выше классификации криптосистем.

Пример 2. 1. Шифр Вернама представляет собой стационарную непараметрическую блочную криптосистему с внешним сеансовым ключом.

2. Шифры Виженера представляют собой стационарные параметрические криптосистемы с предысторией и автоключом, причем роль параметра играет пароль.

3. Шифры DES, AES и ГОСТ 28147-89 представляют собой стационарные блочные параметрические криптосистемы с внешним сеансовым ключом. Для DES и ГОСТ 28147-89 параметром является набор S-блоков, а для AES – набор коэффициентов многочленов.

4. Шифр RSA представляет собой стационарную блочную параметрическую криптосистему с автоключом, причем роль параметра играет набор натуральных чисел.

5. Шифр RC4 представляет собой стационарную поточную параметрическую криптосистему с внешним сеансовым ключом, причем параметр – перестановка чисел 0, 1, …, 255.

6. Нелинейный БПИ-автомат над конечным кольцом [7, 8] представляет собой стационарную поточную параметрическую криптосистему с автоключом, причем параметр – это набор коэффициентов многочленов.

7. Любой квантовый шифр представляет собой криптосистему с предысторией.

Заключение

В работе построена многоосновная алгебраическая система S, предназначенная для исследования современных криптосистем с единых позиций. Дальнейшее, более глубокое исследование абстрактных свойств алгебраической системы S − одно из возможных направлений дальнейших исследований. Второе направление исследований связано с детальной проработкой введенного в работе понятия стационарная (f_j, t_{4j-1}, t_{4j})-криптосистема ($f_j \in F_j$ ($j = 1, 2$), (t_{4j-1}, t_{4j}) $\in T_{f_j}$). Третье направление исследований связано с построением и анализом в рамках алгебраической системы S формальной модели нестационарной криптосистемы. Четвертое направление исследований связано с разработкой в рамках алгебраической системы S формальных моделей пассивных и активных атак криптоаналитика, достаточных для теоретического анализа с единых позиций их эффективности и сложности. Пятое направление исследований связано с разработкой структуры данных, достаточной для эффективного компьютерного моделирования атак криптоаналитика на криптосистемы, определяемые в терминах алгебраической системы S.

ЛИТЕРАТУРА

1. *Алферов А.П.* и др. Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.
2. *Молдовян А.А. и др*. Криптография. Скоростные шифры. СПб.: БХВ-Петербург, 2002. 496 с.
3. *Диффи У*., *Хеллмен М.Е*. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. 1979. Т. 67. № 3. С. 71 – 109.
4. *Месарович М.*, *Такахара Я.* Общая теория систем: математические основы. М.: Мир, 1978. 311 с.
5. *Мальцев А.И*. Алгебраические системы. М.: Наука, 1970. 329 с.
6. *Lynch N*. I/O automaton models and proofs for shared-key communication systems // Proceedings of the 12th IEEE Computer Security Foundations Workshop (CSFW'99), Mordana, Italy, June, 28 – 30, 1999. – 16 p.
7. *Скобелев В.Г*. Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. 2006. № 6. С. 29 – 42.
8. *Скобелев В.Г*. О некоторых свойствах нелинейных БПИ-автоматов над кольцом $\mathbf{Z}_p^k$ // Прикладная радиоэлектроника. 2007. Т. 6. № 2. С. 288 – 299.
9. *Глушков В.М*., *Цейтлин Г.Е*., *Ющенко Е.Л*. Алгебра, языки, программирование. Киев: Наукова думка, 1978. 320 с.