УДК 510.675+519.248+519.712.6

В.В. СКОБЕЛЕВ

СТАТИСТИЧЕСКИ ЭКВИВАЛЕНТНЫЕ ОТОБРАЖЕНИЯ КОНЕЧНЫХ МНОЖЕСТВ

Аннотация. Разработан теоретико-множественный подход, предназначенный для исследования статистически эквивалентных отображений конечного множества. Решены модельные задачи: исследование коллизий отображений, анализ вычислительной стойкости последовательности отображений при условии, что количество аргументов неограниченно возрастает, и вычисление асимптотической вычислительной стойкости этой последовательности отображений, анализ структуры классов статистически эквивалентных отображений, исследования условия статистической эквивалентности отображения и суперпозиции этого отображения с заданным набором отображений.

Ключевые слова: конечные множества, отображения, вычислительная стойкость, статистическая эквивалентность.

ВВЕДЕНИЕ

Одной из актуальных проблем внедрения информационных технологий практически во все сферы жизни современного общества является защита информации. Исследование этой проблемы стимулировало разработку математических основ криптологии [1–4]. Данное направление характеризуется тем, что объектом исследования являются эффективные алгоритмы преобразования конечных структур, построенных на основе моделей дискретной математики и/или конечных алгебраических систем, а предметом исследования — анализ вычислительной стойкости этих алгоритмов. Под эффективностью алгоритма понимается его полиномиальная (временная и емкостная) сложность, а под вычислительной стойкостью — высокая сложность либо успешной идентификации алгоритма (или его параметров), либо успешной имитации его функционирования.

Существуют два основных подхода к анализу вычислительной стойкости алгоритмов: детерминированный и вероятностный. Первый подход [3–7] базируется на анализе сложности идентификации и/или имитации исследуемого алгоритма средствами (т.е. моделями и методами) прикладной теории алгоритмов [8]. Второй подход [2–5, 9, 10], разработанный К. Шенноном в [11], состоит в оценке для данного отображения $f: X \to Y$ следующих двух величин:

- вероятности выбора для фиксированного элемента $y \in Y$ такого элемента $x \in X$, что $f(x) = y$;
- вероятности выбора двух таких элементов $x, x' \in X$ $(x \neq x')$, что истинно равенство $f(x) = f(x')$.

Первая оценка используется, в частности, в качестве меры сложности при идентификации параметров алгоритма на основе его статистического анализа, вторая (ее называют устойчивостью отображения f к коллизиям) — в качестве меры сложности при построении имитационной модели исследуемого алгоритма.

Известно, что мультимножествами [12], определенными на множестве S, называются множества вида $R = \{(s, n(s)) \mid x \in S'\}$, где $S' \subseteq S$, а $n(s) \in \mathbf{Z}_+$ $(s \in S')$ — кратность появления элемента s в мультимножестве R.

Одним из достоинств вероятностного подхода к исследованию вычислительной стойкости алгоритмов является то, что он дает возможность выделять отображения, определенные на конечном множестве и эквивалентные в том смысле, что они имеют одно и то же мультимножество вероятностей выбора значений аргумента, которым соответствует один и тот же элемент, принадлежащий области значений отображения. Естественно назвать такие отображения статистически эквивалентными. Ясно, что они имеют одну и ту же (с вероятностной точки зрения) вычислительную стойкость. Поэтому исследование статистически эквивалентных отображений, определенных на конечных множествах, актуально с теоретической и прикладной точек зрения.

Целью настоящей работы является разработка теоретико-множественного подхода, предназначенного для решения задачи исследования статистически эквивалентных отображений вида $f: X^l \to X$ $(l \in \mathbf{N})$, где X $(|X| \geq 2)$ — конечное множество.

ОСНОВНЫЕ ПОНЯТИЯ

Пусть X $(|X| \geq 2)$ — конечное множество, $\mathsf{F}_l(X)$ $(l \in \mathbf{N})$ — множество всех отображений $f: X^l \to X$,

$$B_f(a) = \{\mathbf{x} \in X^l \mid f(\mathbf{x}) = a\} \quad (f \in \mathsf{F}_l(X), a \in X). \tag{1}$$

Из (1) вытекает, что для каждого отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$:

- $B_f(a) \neq \varnothing$ тогда и только тогда, когда $a \in \mathrm{Val}\, f$;
- $B_f(a_1) \cap B_f(a_2) = \varnothing$ для всех таких $a_1, a_2 \in X$, что $a_1 \neq a_2$;
- $X^l /_{\ker f} = \{B_f(a) \mid a \in \mathrm{Val}\, f\}$.

Положим

$$\mathsf{P}_f(a) = |X|^{-l} \cdot |B_f(a)| \quad (f \in \mathsf{F}_l(X),\ a \in X). \tag{2}$$

Из (1) и (2) вытекает, что для каждого отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$:

- $\mathsf{P}_f(a) \in [0, 1]$ $(a \in X)$;
- $\mathsf{P}_f(a) > 0$ тогда и только тогда, когда $a \in \mathrm{Val}\, f$;
- $\sum\limits_{a \in X} \mathsf{P}_f(a) = 1$.

Таким образом, для каждого отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ отображение $\mathsf{P}_f: X \to [0, 1]$ определяет некоторую вероятностную меру.

Всюду в дальнейшем считаем, что на множестве X задано равномерное распределение вероятностей. При этом предположении истинны следующие два утверждения.

Утверждение 1. Для каждого отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ величина $\mathsf{P}_f(a)$ $(a \in X)$ представляет собой вероятность того, что случайно выбранный набор аргументов $\mathbf{b} \in X^l$ является решением уравнения

$$f(x_1, \ldots, x_l) = a \tag{3}$$

от неизвестных $x_1, \ldots, x_l \in X$.

Утверждение 2. Для каждого отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ множество уравнений $\{f(x_1, \ldots, x_l) = a \mid a \in \mathrm{Val}\, f\}$, имеющих непустое множество решений, разбивается на классы уравнений, эквивалентных в том смысле, что при всех значениях параметра *a*, принадлежащих одному и тому же блоку разбиения $(\mathrm{Val}\, f)/_{\ker \mathsf{P}_f}$, имеет место одна и та же вероятность того, что случайно выбранный набор $\mathbf{b} \in X^l$ — решение уравнения (3).

Утверждения 1 и 2 показывают, что ряд вероятностных характеристик отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ полностью определяется набором величин $\mathsf{P}_f(a)$ $(a \in X)$. Поэтому при исследовании вероятностными методами свойств отображений, принадлежащих множеству $\bigcup\limits_{l=1}^{\infty} \mathsf{F}_l(X)$, важно следующее определение.

Определение 1. Для любых чисел $l_1, l_2 \in \mathbf{N}$ отображения $f_i \in \mathsf{F}_{l_i}(X)$ $(i = 1, 2)$ назовем статистически эквивалентными, если существует такая подстановка $h: X \to X$, что для каждого элемента $a \in X$ истинно равенство

$$\mathsf{P}_{f_1}(a) = \mathsf{P}_{f_2}(h(a)). \tag{4}$$

ПРИМЕРЫ СТАТИСТИЧЕСКИ ЭКВИВАЛЕНТНЫХ ОТОБРАЖЕНИЙ

Пусть $\mathsf{K} = (K, +, \cdot)$ $(|K| \geq 2)$ — конечное ассоциативно-коммутативное кольцо с единицей, а K^{inv} — множество всех обратимых элементов кольца K. Обозначим $\mathsf{F}_l^{(0)}(K)$ $(l \in \mathbf{N})$ множество всех таких отображений $f(x_1, \ldots, x_l) = \sum_{i=1}^{l} a_i x_i + b \in \mathsf{F}_l(K)$, что $a_i \in K^{inv}$ $(i = 1, \ldots, l)$ и $b \in K$. Положим $\mathsf{F}^{(0)}(K) = \bigcup_{l=1}^{\infty} \mathsf{F}_l^{(0)}(K)$.

Лемма 1. Для любого конечного ассоциативно-коммутативного кольца $\mathsf{K} = (K, +, \cdot)$ $(|K| \geq 2)$ с единицей множество $\mathsf{F}^{(0)}(K)$ состоит из статистически эквивалентных отображений.

Доказательство. Докажем лемму индукцией по числу $l \in \mathbf{N}$.

Пусть $l = 1$. Для каждого отображения $f(x_1) = a_1 x_1 + b \in \mathsf{F}_1^{(0)}(K)$ $(a_1 \in K^{inv}$, $b \in K)$ и каждого элемента $a \in K$ имеем $x_1 \in B_f(a) \Leftrightarrow a_1 x_1 + b = a \Leftrightarrow x_1 = a_1^{-1}(a - b)$, т.е. $|B_f(a)| = 1$ для всех элементов $a \in K$. Следовательно, из (2) вытекает, что для каждого отображения $f \in \mathsf{F}_1^{(0)}(K)$ истинны равенства

$$\mathsf{P}_f(a) = |K|^{-1} \quad (a \in K). \tag{5}$$

Таким образом, для любых отображений $f_1, f_2 \in \mathsf{F}_1^{(0)}(K)$ равенство $\mathsf{P}_{f_1}(a) = \mathsf{P}_{f_2}(a)$ истинно для всех элементов $a \in K$ (т.е. $h: K \to K$ — тождественная подстановка). Следовательно, множество $\mathsf{F}_1^{(0)}(K)$ состоит из статистически эквивалентных отображений.

Предположим, что для числа $l \in \mathbf{N}$ множество $\bigcup_{j=1}^{l} \mathsf{F}_j^{(0)}(K)$ состоит из статистически эквивалентных отображений.

Поскольку каждое отображение, принадлежащее множеству $\bigcup_{j=2}^{l} \mathsf{F}_j^{(0)}(K)$, статистически эквивалентно некоторому отображению, принадлежащему множеству $\mathsf{F}_1^{(0)}(K)$, для каждого отображения $f \in \bigcup_{j=1}^{l} \mathsf{F}_j^{(0)}(K)$ истинны равенства (5).

Докажем, что множество $\bigcup_{j=1}^{l+1} \mathsf{F}_j^{(0)}(K)$ состоит из статистически эквивалентных отображений. Для этого достаточно доказать, что каждое отображение, принадлежащее множеству $\mathsf{F}_{l+1}^{(0)}(K)$, статистически эквивалентно некоторому отображению, принадлежащему множеству $\bigcup_{j=1}^{l} \mathsf{F}_j^{(0)}(K)$, т.е. что для каждого отображения $f \in \mathsf{F}_{l+1}^{(0)}(K)$ истинны равенства (5).

Для каждого отображения $f(x_1, \ldots, x_{l+1}) = \sum_{i=1}^{l+1} a_i x_i + b \in \mathsf{F}_{l+1}^{(0)}(K)$ $(a_i \in K^{inv}$ $(i = 1, \ldots, l+1)$ и $b \in K)$ и каждого элемента $a \in K$ получим, что

$$(x_1, \ldots, x_{l+1}) \in B_f(a) \Leftrightarrow \sum_{i=1}^{l+1} a_i x_i + b = a \Leftrightarrow x_1 = a_1^{-1}\left(a - b - \sum_{i=2}^{l+1} a_i x_i\right).$$

Следовательно,

$$B_f(a) = \left\{\left(a_1^{-1}\left(a - b - \sum_{i=2}^{l+1} a_i x_i\right), x_2, \ldots, x_{l+1}\right) \mid x_2, \ldots, x_{l+1} \in K\right\} \quad (a \in K),$$

т.е. $|B_f(a)|=|K|^l$ для каждого элемента $a\in K$. Поэтому из (2) вытекает, что для каждого отображения $f\in \mathsf{F}_{l+1}^{(0)}(K)$ и всех элементов $a\in K$ имеем $\mathsf{P}_f(a)=|K|^{-(l+1)}\cdot|B_f(a)|=|K|^{-(l+1)}\cdot|K|^l=|K|^{-1}$, т.е. для каждого отображения $f\in \mathsf{F}_{l+1}^{(0)}(K)$ истинны равенства (5), что и требовалось доказать.

Итак, показано, что для каждого числа $l\in\mathbf{N}$ множество $\bigcup_{j=1}^{l}\mathsf{F}_j^{(0)}(K)$ состоит из статистически эквивалентных отображений. Отсюда непосредственно вытекает, что множество $\mathsf{F}^{(0)}(K)=\bigcup_{l=1}^{\infty}\mathsf{F}_l^{(0)}(K)$ состоит из статистически эквивалентных отображений.

Лемма доказана.

Известно, что классами ассоциированных элементов кольца вычетов $\mathsf{Z}_{p^k}=(\mathbf{Z}_{p^k},+,\cdot)$, где p — простое число, а $k\in\mathbf{N}$ ($k\ge 2$), являются множества $C_0=\{0\}$, $C_1=\mathbf{Z}_{p^k}^{inv}$ и $C_i=\{\alpha\cdot p^i\mid\alpha\in\mathbf{Z}_{p^k}^{inv}\}$ $(i=1,\dots,k-1)$. Рассмотрим подмножество $\widetilde{\mathsf{F}}_1(\mathbf{Z}_{p^k})=\{f_\beta|\,\beta\in\mathbf{Z}_{p^k}^{inv}\}$ множества отображений $\mathsf{F}_1(\mathbf{Z}_{p^k})$, где

$$f_\beta(x)=\begin{cases}0, & \text{если } x\in C_0,\\ 1, & \text{если } x\in C_1,\\ \beta\cdot p^i, & \text{если } x\in C_i\ (i=1,\dots,k-1)\end{cases}\qquad (\beta\in\mathbf{Z}_{p^k}^{inv}). \tag{6}$$

Лемма 2. Для любого кольца вычетов $\mathsf{Z}_{p^k}=(\mathbf{Z}_{p^k},+,\cdot)$, где p — простое число, а $k\in\mathbf{N}$ ($k\ge 2$), множество $\widetilde{\mathsf{F}}_1(\mathbf{Z}_{p^k})$ состоит из статистически эквивалентных отображений.

Доказательство. Из равенства (6) получаем, что для каждого отображения $f_\beta\in\widetilde{\mathsf{F}}_1(\mathbf{Z}_{p^k})$ $(\beta\in\mathbf{Z}_{p^k}^{inv})$ истинно равенство

$$B_{f_\beta}(a)=\begin{cases}C_0, & \text{если } a=0,\\ C_1, & \text{если } a=1,\\ C_i, & \text{если } a=\beta\cdot p^i\ \ (i=1,\dots,k-1),\\ \varnothing, & \text{если } a\in\mathbf{Z}_{p^k}\setminus(\{0,1\}\cup\{\beta\cdot p^i\mid i=1,\dots,k-1\}).\end{cases}$$

Из (2) вытекает, что для каждого отображения $f\in\mathsf{F}_1^{(0)}(K)$

$$\mathsf{P}_{f_\beta}(a)=\begin{cases}|\mathbf{Z}_{p^k}|^{-1}\cdot|C_0|, & \text{если } a=0,\\ |\mathbf{Z}_{p^k}|^{-1}\cdot|C_1|, & \text{если } a=1,\\ |\mathbf{Z}_{p^k}|^{-1}\cdot|C_i|, & \text{если } a=\beta\cdot p^i\ \ (i=1,\dots,k-1),\\ 0, & \text{если } a\in\mathbf{Z}_{p^k}\setminus(\{0,1\}\cup\{\beta\cdot p^i|\,i=1,\dots,k-1\}).\end{cases}$$

Таким образом, для любых отображений $f_{\beta_1},f_{\beta_2}\in\widetilde{\mathsf{F}}_1(\mathbf{Z}_{p^k})$ $(\beta_1,\beta_2\in\mathbf{Z}_{p^k}^{inv})$ истинны равенства

$$\mathsf{P}_{f_{\beta_1}}(0)=\mathsf{P}_{f_{\beta_2}}(0)=|\mathbf{Z}_{p^k}|^{-1}\cdot|C_0|,$$
$$\mathsf{P}_{f_{\beta_1}}(1)=\mathsf{P}_{f_{\beta_2}}(1)=|\mathbf{Z}_{p^k}|^{-1}\cdot|C_1|,$$
$$\mathsf{P}_{f_{\beta_1}}(\beta_1\cdot p^i)=\mathsf{P}_{f_{\beta_2}}(\beta_2\cdot p^i)=|\mathbf{Z}_{p^k}|^{-1}\cdot|C_i|\ \ (i=1,\dots,k-1),$$
$$\mathsf{P}_{f_{\beta_1}}(a)=\mathsf{P}_{f_{\beta_2}}(a)=0\ \left(a\in\mathbf{Z}_{p^k}\setminus\left(\{0,1\}\cup\bigcup_{j=1}^{2}\{\beta_j\cdot p^i|\ i=1,\dots,k-1\}\right)\right).$$

Следовательно, для подстановки $h_{\beta_1,\beta_2}:\mathbf{Z}_{p^k}\to\mathbf{Z}_{p^k}$, определенной равенством

$$h_{\beta_1,\beta_2}(a)=\begin{cases}\beta_2\cdot\beta_1^{-1}\cdot a, & \text{если } a=\beta_1\cdot p^i \ (i=1,\ldots,k-1),\\ \beta_1\cdot\beta_2^{-1}\cdot a, & \text{если } a=\beta_2\cdot p^i \ (i=1,\ldots,k-1),\\ a, & \text{если } a\in\mathbf{Z}_{p^k}\setminus\bigcup_{j=1}^{2}\{\beta_i\cdot p^i\,|\,i=1,\ldots,k-1\},\end{cases}$$

равенство $\mathsf{P}_{f_{\beta_1}}(a)=\mathsf{P}_{f_{\beta_2}}(h_{\beta_1,\beta_2}(a))$ истинно для всех элементов $a\in\mathbf{Z}_{p^k}$. Отсюда вытекает, что множество $\widetilde{\mathsf{F}}_1(\mathbf{Z}_{p^k})$ состоит из статистически эквивалентных отображений.

Лемма доказана.

УСТОЙЧИВОСТЬ ОТОБРАЖЕНИЙ К КОЛЛИЗИЯМ

Для каждого отображения $f\in\mathsf{F}_l(X)$ $(l\in\mathbf{N})$ обозначим $\widehat{\mathsf{P}}_f$ $(\breve{\mathsf{P}}_f)$ вероятность того, что при выборе с возвращением (без возвращения) для случайно выбранных наборов $\mathbf{b}_1,\mathbf{b}_2\in X^l$ выполнено условие $\mathbf{b}_1\neq\mathbf{b}_2$ и $f(\mathbf{b}_1)=f(\mathbf{b}_2)$ (условие $f(\mathbf{b}_1)=f(\mathbf{b}_2)$).

Теорема 1. Для каждого отображения $f\in\mathsf{F}_l(X)$ $(l\in\mathbf{N})$ истинны равенства

$$\widehat{\mathsf{P}}_f=(1+|X|^{-l})^{-1}\left(\sum_{a\in\mathrm{Val}\,f}\mathsf{P}_f^2(a)-|X|^{-l}\right),\tag{7}$$

$$\breve{\mathsf{P}}_f=(1-|X|^{-l})^{-1}\left(\sum_{a\in\mathrm{Val}\,f}\mathsf{P}_f^2(a)-|X|^{-l}\right).\tag{8}$$

Доказательство. Рассмотрим произвольное отображение $f\in\mathsf{F}_l(X)$ $(l\in\mathbf{N})$.

Если осуществляется выбор с возвращением, то для каждого элемента $a\in\mathrm{Val}\,f$ вероятность того, что $\mathbf{b}_1\neq\mathbf{b}_2$ и $f(\mathbf{b}_1)=f(\mathbf{b}_2)=a$ для случайно выбранных наборов $\mathbf{b}_1,\mathbf{b}_2\in X^l$, имеет вид

$$\widehat{\mathsf{P}}_f(a)=C^2_{|B_f(a)|}(C^2_{|X|^l}+|X|^l)^{-1},\tag{9}$$

где C_n^m — число сочетаний из n элементов по m элементам.

Если осуществляется выбор без возвращения, то для каждого элемента $a\in\mathrm{Val}\,f$ вероятность того, что $f(\mathbf{b}_1)=f(\mathbf{b}_2)=a$ для случайно выбранных наборов $\mathbf{b}_1,\mathbf{b}_2\in X^l$, имеет вид

$$\breve{\mathsf{P}}_f(a)=C^2_{|B_f(a)|}(C^2_{|X|^l})^{-1}.\tag{10}$$

Из (2) и (9) вытекает, что для каждого элемента $a\in\mathrm{Val}\,f$

$$\widehat{\mathsf{P}}_f(a)=\frac{0{,}5|B_f(a)|(|B_f(a)|-1)}{0{,}5|X|^l(|X|^l+1)}=\frac{|B_f(a)|}{|X|^l}\left(\frac{|B_f(a)|}{|X|^l}-\frac{1}{|X|^l}\right)\left(1+\frac{1}{|X|^l}\right)^{-1}=$$

$$=\mathsf{P}_f(a)(\mathsf{P}_f(a)-|X|^{-l})(1+|X|^{-l})^{-1}.\tag{11}$$

Из (2) и (10) вытекает, что для каждого элемента $a\in\mathrm{Val}\,f$

$$\breve{\mathsf{P}}_f(a)=\frac{0{,}5|B_f(a)|(|B_f(a)|-1)}{0{,}5|X|^l(|X|^l-1)}=\frac{|B_f(a)|}{|X|^l}\left(\frac{|B_f(a)|}{|X|^l}-\frac{1}{|X|^l}\right)\left(1-\frac{1}{|X|^l}\right)^{-1}=$$

$$=\mathsf{P}_f(a)(\mathsf{P}_f(a)-|X|^{-l})(1-|X|^{-l})^{-1}.\tag{12}$$

Поскольку $\widehat{\mathsf{P}}_f = \sum_{a\in \mathrm{Val}\, f} \widehat{\mathsf{P}}_f(a)$, воспользовавшись равенством (11), получим

$$\widehat{\mathsf{P}}_f = \sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f(a)(\mathsf{P}_f(a) - |X|^{-l})(1+|X|^{-l})^{-1} =$$

$$= (1+|X|^{-l})^{-1}\left(\sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f^2(a) - |X|^{-l} \sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f(a)\right) =$$

$$= (1+|X|^{-l})^{-1}\left(\sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f^2(a) - |X|^{-l}\cdot 1\right) =$$

$$= (1+|X|^{-l})^{-1}\left(\sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f^2(a) - |X|^{-l}\right),$$

что и требовалось доказать.

Поскольку $\breve{\mathsf{P}}_f = \sum_{a\in \mathrm{Val}\, f} \breve{\mathsf{P}}_f(a)$, воспользовавшись равенством (12), получим

$$\breve{\mathsf{P}}_f = \sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f(a)(\mathsf{P}_f(a) - |X|^{-l})(1-|X|^{-l})^{-1} =$$

$$= (1-|X|^{-l})^{-1}\left(\sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f^2(a) - |X|^{-l} \sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f(a)\right) =$$

$$= (1-|X|^{-l})^{-1}\left(\sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f^2(a) - |X|^{-l}\cdot 1\right) =$$

$$= (1-|X|^{-l})^{-1}\left(\sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f^2(a) - |X|^{-l}\right),$$

что и требовалось доказать.

Теорема доказана.

Следствие 1. Для каждого отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ истинны неравенства

$$\widehat{\mathsf{P}}_f \ge (1+|X|^{-l})^{-1}(|\mathrm{Val} f|^{-1} - |X|^{-l}), \tag{13}$$

$$\breve{\mathsf{P}}_f \ge (1-|X|^{-l})^{-1}(|\mathrm{Val} f|^{-1} - |X|^{-l}). \tag{14}$$

Доказательство. Известно, что для каждого числа $n \in \mathbf{N}$ $(n \ge 2)$, если выполнены условия $0 < u_i < 1$ $(i = 1, \ldots, n)$ и $\sum_{i=1}^{n} u_i = 1$, то выражение $\sum_{i=1}^{n} u_i^2$ принимает наименьшее значение тогда и только тогда, когда $u_i = n^{-1}$ для всех $i = 1, \ldots, n$. Следовательно, выражение $\sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f^2(a)$ принимает наименьшее значение тогда и только тогда, когда $\mathsf{P}_f(a) = |\mathrm{Val} f|^{-1}$ для всех $a \in \mathrm{Val} f$. При этом

$$\sum_{a\in \mathrm{Val}\, f} \mathsf{P}_f^2(a) = \sum_{a\in \mathrm{Val}\, f} |\mathrm{Val} f|^{-2} = |\mathrm{Val} f| \cdot |\mathrm{Val} f|^{-2} = |\mathrm{Val} f|^{-1}.$$

Отсюда и из равенств (7) и (8) вытекает, что неравенства (10) и (11) истинны для каждого отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$.

Следствие доказано.

ВЫЧИСЛИТЕЛЬНАЯ СТОЙКОСТЬ ПОСЛЕДОВАТЕЛЬНОСТИ ОТОБРАЖЕНИЙ

При анализе задач защиты информации под сложностью алгоритма A естественно понимать величину $\max\{T_A, V_A\}$, где T_A и V_A — соответственно время и объем памяти, необходимые для вычисления согласно алгоритму A. Действительно, быстрый алгоритм A, применяемый для защиты информации, характеризуется тем, что величина $\max\{T_A, V_A\}$ ограничена сверху полиномом невысокой степени от размера входа. Эффективный алгоритм A (если такой существует) атаки на алгоритм защиты информации характеризуется тем, что величина $\max\{T_A, V_A\}$ ограничена сверху полиномом от размера входа.

Известно, что модельной задачей защиты информации является построение для достаточно большого по мощности конечного множества X последовательности отображений $f_l \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$, предназначенной для вычисления (возможно, открытого) ключа $a \in X$ по секретному ключу $\mathbf{b} \in X^l$. Оценим вычислительную стойкость этой последовательности отображений относительно атак, построенных на основе использования вероятностных методов, при выполнении следующих двух условий.

Условие 1. Существуют такие константы $c_1, c_2 \in [1-\varepsilon_1; 1]$ $(c_1 < c_2)$, где ε_1 — достаточно малое положительное число, что при каждом значении $l \in \mathbf{N}$ истинны неравенства

$$c_1 |X| \le |\mathrm{Val}\, f_l| \le c_2 |X|. \tag{15}$$

Условие 2. Существуют такие константы $c_3, c_4 \in [1-\varepsilon_2; 1+\varepsilon_2]$ $(c_3 < c_4)$, где ε_2 — достаточно малое положительное число, что при каждом значении $l \in \mathbf{N}$ для всех $a \in \mathrm{Val} f_l$ истинны неравенства

$$c_3 |\mathrm{Val}\, f_l|^{-1} \le \mathsf{P}_{f_l}(a) \le c_4 |\mathrm{Val}\, f_l|^{-1}. \tag{16}$$

Лемма 3. Если для последовательности $f_l \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ выполнены условия 1 и 2, то при каждом значении $l \in \mathbf{N}$ истинны неравенства

$$(1-\varepsilon_2)|X|^{-1} \le \mathsf{P}_{f_l}(a) \le (1-\varepsilon_1)^{-1}(1+\varepsilon_2)|X|^{-1}. \tag{17}$$

Доказательство. Предположим, что для последовательности $f_l \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ выполнены условия 1 и 2.

Из неравенств (15) вытекает, что при каждом значении $l \in \mathbf{N}$

$$c_2^{-1}|X|^{-1} \le |\mathrm{Val}\, f_l|^{-1} \le c_1^{-1}|X|^{-1}. \tag{18}$$

Из неравенств (16) и (18) вытекает, что при каждом значении $l \in \mathbf{N}$

$$c_2^{-1}c_3|X|^{-1} \le \mathsf{P}_{f_l}(a) \le c_1^{-1}c_4|X|^{-1}. \tag{19}$$

Так как $c_1, c_2 \in [1-\varepsilon_1; 1]$ и $c_3, c_4 \in [1-\varepsilon_2; 1+\varepsilon_2]$, то $c_2^{-1}c_3 \ge 1-\varepsilon_2$ и $0 < c_1^{-1}c_4 \le$ $\le (1-\varepsilon_1)^{-1}(1+\varepsilon_2)$. Воспользовавшись этими неравенствами из (19), получим, что неравенства (17) истинны при каждом значении $l \in \mathbf{N}$.

Лемма доказана.

Теорема 2. Если для последовательности $f_l \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ выполнены условия 1 и 2, то при каждом значении $l \in \mathbf{N}$ истинны неравенства

$$\begin{gathered}(1+|X|^{-l})^{-1}((1-\varepsilon_2)^2(1-\varepsilon_1)|X|^{-1} - |X|^{-l}) \le \widehat{\mathsf{P}}_{f_l} \le \\ \le (1+|X|^{-l})^{-1}((1-\varepsilon_1)^{-2}(1+\varepsilon_2)^2|X|^{-1} - |X|^{-l}),\end{gathered} \tag{20}$$

$$\begin{gathered}(1-|X|^{-l})^{-1}((1-\varepsilon_2)^2(1-\varepsilon_1)|X|^{-1} - |X|^{-l}) \le \breve{\mathsf{P}}_{f_l} \le \\ \le (1-|X|^{-l})^{-1}((1-\varepsilon_1)^{-2}(1+\varepsilon_2)^2|X|^{-1} - |X|^{-l}).\end{gathered} \tag{21}$$

Доказательство. Предположим, что для последовательности $f_l \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ выполнены условия 1 и 2.

Из неравенств (17) вытекает, что при каждом значении $l \in \mathbf{N}$

$$(1-\varepsilon_2)^2|X|^{-2} \le \mathsf{P}_{f_l}^2(a) \le (1-\varepsilon_1)^{-2}(1+\varepsilon_2)^2|X|^{-2}.$$

Следовательно, при каждом значении $l \in \mathbf{N}$

$$(1-\varepsilon_2)^2 \mid X \mid^{-2} \mid \mathrm{Val}\, f_l \mid \le \sum_{a \in \mathrm{Val}\, f_l} \mathsf{P}^2_{f_l}(a) \le (1-\varepsilon_1)^{-2} (1+\varepsilon_2)^2 \mid X \mid^{-2} \mid \mathrm{Val}\, f_l \mid . \quad (22)$$

Подставив в (22) неравенства (15), получим, что при каждом значении $l \in \mathbf{N}$

$$(1-\varepsilon_2)^2 c_1 \mid X \mid^{-1} \le \sum_{a \in \mathrm{Val}\, f_l} \mathsf{P}^2_{f_l}(a) \le (1-\varepsilon_1)^{-2} (1+\varepsilon_2)^2 c_2 \mid X \mid^{-1}. \quad (23)$$

Так как $c_1, c_2 \in [1-\varepsilon_1; 1]$, то $c_1 \ge 1-\varepsilon_1$ и $0 < c_2 \le 1$. Воспользовавшись этими неравенствами из (23), получим, что при каждом значении $l \in \mathbf{N}$

$$(1-\varepsilon_2)^2 (1-\varepsilon_1) \mid X \mid^{-1} \le \sum_{a \in \mathrm{Val}\, f_l} \mathsf{P}^2_{f_l}(a) \le (1-\varepsilon_1)^{-2} (1+\varepsilon_2)^2 \mid X \mid^{-1}. \quad (24)$$

Из (24) и (7), (8) вытекает, что неравенства (20) и (21) истинны при каждом значении $l \in \mathbf{N}$.

Теорема доказана.

Из теоремы 2 непосредственно вытекает, что истинно следующее следствие.

Следствие 2. Если для последовательности $f_l \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ выполнены условия 1 и 2, то истинны неравенства

$$(1-\varepsilon_2)^2 (1-\varepsilon_1) \mid X \mid^{-1} \le \lim_{l \to \infty} \widehat{\mathsf{P}}_{f_l} \le (1-\varepsilon_1)^{-2} (1+\varepsilon_2)^2 \mid X \mid^{-1}, \quad (25)$$

$$(1-\varepsilon_2)^2 (1-\varepsilon_1) \mid X \mid^{-1} \le \lim_{l \to \infty} \breve{\mathsf{P}}_{f_l} \le (1-\varepsilon_1)^{-2} (1+\varepsilon_2)^2 \mid X \mid^{-1}. \quad (26)$$

Ясно, что если $f_l^{(1)} \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ и $f_l^{(2)} \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ — такие последовательности отображений, что для каждого значения $l \in \mathbf{N}$ отображения $f_l^{(1)}$ и $f_l^{(2)}$ статистически эквивалентны, то эти последовательности имеют одну и ту же вычислительную стойкость относительно атак, построенных на основе использования вероятностных методов. Отсюда вытекает, что для задач защиты информации актуально исследование классов статистически эквивалентных отображений $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$.

КЛАССЫ СТАТИСТИЧЕСКИ ЭКВИВАЛЕНТНЫХ ОТОБРАЖЕНИЙ

Говорят, что разбиение n-элементного множества имеет тип $(k_1, \ldots, k_n)$ $(\sum_{i=1}^{n} i k_i = n)$, если оно содержит k_i $(i = 1, \ldots, n)$ i-элементных блоков. Определим аналогичное понятие для отображений $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$.

Определение 2. Отображение $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ имеет тип $(k_1, \ldots, k_{|X|^l})$, если фактор-множество $X^l /_{\ker f} = \{B_f(a) \mid a \in \mathrm{Val} f\}$, рассматриваемое как разбиение множества X^l, имеет тип $(k_1, \ldots, k_{|X|^l})$.

Из определения 2 вытекает, что для отображения $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$, имеющего тип $(k_1, \ldots, k_{|X|^l})$, истинно равенство $\sum_{i=1}^{|X|^l} k_i = \mid \mathrm{Val} f \mid$. Поэтому типами отображений $f \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ являются такие и только такие наборы $(k_1, \ldots, k_{|X|^l})$, которые удовлетворяют следующим трем условиям:

- $k_i \in \mathbf{Z}_+$ для всех $i = 1, \ldots, \mid X \mid^l$;
- $\sum_{i=1}^{|X|^l} i k_i = \mid X \mid^l$;
- $1 \le \sum_{i=1}^{|X|^l} k_i \le \mid X \mid$.

Теорема 3. Отображения $f_1, f_2 \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ являются статистически эквивалентными тогда и только тогда, когда отображения f_1 и f_2 имеют один и тот же тип.

Доказательство. Зафиксируем число $l \in \mathbf{N}$.

Пусть $f_1, f_2 \in \mathsf{F}_l(X)$ — статистически эквивалентные отображения. Докажем, что отображения f_1 и f_2 имеют один и тот же тип.

Поскольку $f_1, f_2 \in \mathsf{F}_l(X)$ — статистически эквивалентные отображения, существует такая подстановка $h: X \to X$, что равенство $\mathsf{P}_{f_1}(a) = \mathsf{P}_{f_2}(h(a))$ истинно для всех элементов $a \in X$. Следовательно, из (2) вытекает, что для всех элементов $a \in \mathrm{Val}\, f$

$$|X|^{-l} \cdot |B_{f_1}(a)| = |X|^{-l} \cdot |B_{f_2}(h(a))| \Leftrightarrow |B_{f_1}(a)| = |B_{f_2}(h(a))|.$$

Так как $\sum_{a \in \mathrm{Val}\, f_1} |B_{f_1}(a)| = |X|^l$, $h: X \to X$ — подстановка и $|B_{f_1}(a)| = |B_{f_2}(h(a))|$ для всех элементов $a \in \mathrm{Val}\, f_1$, то $\sum_{a \in \mathrm{Val}\, f_1} |B_{f_2}(h(a))| = |X|^l$. Поэтому $\mathrm{Val}\, f_2 = \{h(a) \mid a \in \mathrm{Val} f_1\}$. Отсюда вытекает, что разбиения $X^l/_{\ker f_1} = \{B_{f_1}(a) \mid a \in \mathrm{Val}\, f_1\}$ и $X^l/_{\ker f_2} = \{B_{f_2}(h(a)) \mid a \in \mathrm{Val}\, f_1\} = \{B_{f_2}(b) \mid b \in \mathrm{Val}\, f_2\}$ множества X^l имеют один и тот же тип, что и требовалось доказать.

Пусть отображения $f_1, f_2 \in \mathsf{F}_l(X)$ имеют один и тот же тип $(k_1, \ldots, k_{|X|^l})$. Докажем, что отображения f_1 и f_2 являются статистически эквивалентными.

Положим $I_{f_1, f_2} = \{i \in \{1, \ldots, |X|^l\} \mid k_i > 0\}$. Для каждого числа $i \in I_{f_1, f_2}$ построим k_i-элементные множества $S_1(i) = \{a \in X \mid |B_{f_1}(a)| = i\}$ и $S_2(i) = \{b \in X \mid |B_{f_2}(b)| = i\}$. Ясно, что множества $S_1(i)$ $(i \in I_{f_1, f_2})$ и $S_2(i)$ $(i \in I_{f_1, f_2})$ попарно не пересекаются.

Зафиксируем такие биекции $h_i: S_1(i) \to S_2(i)$ $(i \in I_{f_1, f_2})$, что $h_i(a) = a$ для всех $a \in S_1(i) \cap S_2(i)$ и определим подстановку $h: X \to X$ следующим образом:

$$h(a) = \begin{cases} h_i(a), & \text{если } a \in S_1(i) \setminus S_2(i) \text{ для некоторого } i \in I_{f_1, f_2}, \\ h_i^{-1}(a), & \text{если } a \in S_2(i) \setminus S_1(i) \text{ для некоторого } i \in I_{f_1, f_2}, \\ a & \text{в остальных случаях.} \end{cases}$$

Из определения множеств $S_1(i)$ $(i \in I_{f_1, f_2})$, $S_2(i)$ $(i \in I_{f_1, f_2})$, биекций h_i $(i \in I_{f_1, f_2})$ и подстановки $h: X \to X$, вытекает, что равенство $|B_{f_1}(a)| = |B_{f_2}(h(a))|$ истинно для всех элементов $a \in X$. Следовательно, равенство $\mathsf{P}_{f_1}(a) = \mathsf{P}_{f_2}(h(a))$ истинно для всех элементов $a \in X$, т.е. отображения f_1 и f_2 являются статистически эквивалентными, что и требовалось доказать.

Теорема доказана.

Из теоремы 3 вытекает, что для каждого числа $l \in \mathbf{N}$ разбиение множества $\mathsf{F}_l(X)$ на классы статистически эквивалентных отображений имеет вид

$$\pi(X, l) = \left\{ C(k_1, \ldots, k_{|X|^l}) \mid k_i \in \mathbf{Z}_+ (i = 1, \ldots, |X|^l) \ \& \ \sum_{i=1}^{|X|^l} i k_i = |X|^l \ \& \ 1 \le \sum_{i=1}^{|X|^l} k_i \le |X| \right\},$$

где $C(k_1, \ldots, k_{|X|^l})$ — множество всех отображений $f \in \mathsf{F}_l(X)$, имеющих тип $(k_1, \ldots, k_{|X|^l})$.

Теорема 4. Для каждого числа $l \in \mathbf{N}$ равенства

$$|C(k_1, \ldots, k_{|X|^l})| = \frac{|X|! \cdot (|X|^l)!}{\left(|X| - \sum_{i=1}^{|X|^l} k_i\right)! \cdot \prod_{i=1}^{|X|^l} ((i!)^{k_i} k_i!)} \tag{27}$$

истинны для всех таких наборов $(k_1, \dots, k_{|X|^l})$, что $k_i \in \mathbf{Z}_+$ $(i = 1, \dots, |X|^l)$, $\sum_{i=1}^{|X|^l} ik_i = |X|^l$ и $1 \le \sum_{i=1}^{|X|^l} k_i \le |X|$.

Доказательство. Зафиксируем число $l \in \mathbf{N}$ и такой набор $(k_1, \dots, k_{|X|^l})$, что $k_i \in \mathbf{Z}_+$ $(i = 1, \dots, |X|^l)$, $\sum_{i=1}^{|X|^l} ik_i = |X|^l$ и $1 \le \sum_{i=1}^{|X|^l} k_i \le |X|$.

Обозначим $B(k_1, \dots, k_{|X|^l})$ множество всех разбиений множества X^l, имеющих тип $(k_1, \dots, k_{|X|^l})$, и положим $\mathsf{S}(\pi) = \{ f \in \mathsf{F}_l(X) \mid X^l /_{\ker f} = \pi \}$ $(\pi \in B(k_1, \dots, k_{|X|^l}))$.

Так как $\{\mathsf{S}(\pi) \mid \pi \in B(k_1, \dots, k_{|X|^l})\}$ — разбиение множества $C(k_1, \dots, k_{|X|^l})$, то

$$|C(k_1, \dots, k_{|X|^l})| = \sum_{\pi \in B(k_1, \dots, k_{|X|^l})} |\mathsf{S}(\pi)|. \tag{28}$$

Для каждого разбиения $\pi \in B(k_1, \dots, k_{|X|^l})$ число $|\mathsf{S}(\pi)|$ равно числу всех биекций фиксированного $|X^l /_{\ker f}|$-элементного множества на всевозможные $\sum_{i=1}^{|X|^l} k_i$-элементные подмножества множества X. Следовательно,

$$|\mathsf{S}(\pi)| = \frac{|X|!}{\left(|X| - \sum_{i=1}^{|X|^l} k_i\right)!} \quad (\pi \in B(k_1, \dots, k_{|X|^l})). \tag{29}$$

Число всех разбиений n-элементного множества, имеющих тип $(k_1, \dots, k_n)$ $(\sum_{i=1}^{n} ik_i = n)$, равно $\dfrac{n!}{\prod_{i=1}^{n} (i!)^{k_i} k_i!}$. Следовательно,

$$|B(k_1, \dots, k_{|X|^l})| = \frac{(|X|^l)!}{\prod_{i=1}^{|X|^l} (i!)^{k_i} k_i!}. \tag{30}$$

Из (28)–(30) вытекает, что

$$|C(k_1, \dots, k_{|X|^l})| = \sum_{\pi \in B(k_1, \dots, k_{|X|^l})} |\mathsf{S}(\pi)| = \sum_{\pi \in B(k_1, \dots, k_{|X|^l})} \frac{|X|!}{\left(|X| - \sum_{i=1}^{|X|^l} k_i\right)} =$$

$$= \frac{|X|!}{\left(|X| - \sum_{i=1}^{|X|^l} k_i\right)} \cdot \sum_{\pi \in B(k_1, \dots, k_{|X|^l})} 1 = \frac{|X|!}{\left(|X| - \sum_{i=1}^{|X|^l} k_i\right)} \cdot |B(k_1, \dots, k_{|X|^l})| =$$

$$= \frac{|X|!}{\left(|X| - \sum_{i=1}^{|X|^l} k_i\right)!} \cdot \frac{(|X|^l)!}{\prod_{i=1}^{|X|^l} ((i!)^{k_i} k_i!)} = \frac{|X|! \cdot (|X|^l)!}{\left(|X| - \sum_{i=1}^{|X|^l} k_i\right)! \cdot \prod_{i=1}^{|X|^l} ((i!)^{k_i} k_i!)}.$$

Теорема доказана.

Следствие 3. Для каждого числа $l \in \mathbf{N}$ число $n_{c_3, c_4}(l)$ отображений $f_l \in \mathsf{F}_l(X)$, имеющих тип $(k_1, \dots, k_{|X|^l})$ и удовлетворяющих условию 1, равно

$$n_{c_3, c_4}(l) = \sum_{j = \lceil c_1 |X| \rceil}^{\lfloor c_2 |X| \rfloor} \frac{|X|! \cdot (|X|^l)!}{(|X| - j)! \cdot \prod_{i=1}^{|X|^l} ((i!)^{k_i} k_i!)}. \tag{31}$$

Доказательство. Для любого отображения $f_l \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$, имеющего тип $(k_1, \ldots, k_{|X|^l})$, истинно равенство $\sum_{i=1}^{|X|^l} k_i = |\operatorname{Val} f|$. Поэтому из неравенств (15) и равенства (27) вытекает, что равенство (31) истинно.

Следствие доказано.

СУПЕРПОЗИЦИИ ОТОБРАЖЕНИЙ

Пусть $f \in \mathsf{F}_m(X)$ $(m \in \mathbf{N})$ и $\varphi_i \in \mathsf{F}_l(X)$ $(l \in \mathbf{N})$ для всех $i = 1, \ldots, m$. Суперпозиция отображения $f(t_1, \ldots, t_m)$ и набора отображений $\varphi_i(x_1, \ldots, x_l)$ $(i = 1, \ldots, m)$ определяется равенством $g(x_1, \ldots, x_l) = f(\varphi_1(x_1, \ldots, x_l), \ldots, \varphi_m(x_1, \ldots, x_l))$.

Ясно, что для суперпозиции $g \in \mathsf{F}_l(X)$ любого отображения $f \in \mathsf{F}_m(X)$ и любого набора отображений $\varphi_i \in \mathsf{F}_l(X)$ $(i = 1, \ldots, m)$ имеет место включение $\operatorname{Va}l\, g \subseteq \operatorname{Val} f$. Отсюда непосредственно вытекает, что истинно следующее утверждение.

Утверждение 3. Суперпозиция $g \in \mathsf{F}_l(X)$ отображения $f \in \mathsf{F}_m(X)$ и набора отображений $\varphi_i \in \mathsf{F}_l(X)$ $(i = 1, \ldots, m)$ не является статистически эквивалентной отображению f, если $\operatorname{Val} g \subset \operatorname{Val} f$.

Рассмотрим ситуацию, когда для суперпозиции $g \in \mathsf{F}_l(X)$ отображения $f \in \mathsf{F}_m(X)$ и набора отображений $\varphi_i \in \mathsf{F}_l(X)$ $(i = 1, \ldots, m)$ имеет место равенство

$$\operatorname{Va}l\, g = \operatorname{Val} f. \tag{32}$$

Разбиение $\pi = \bigcap_{i=1}^{m} (X^l /_{\ker \varphi_i})$ множества X^l удовлетворяет условию

$$(a_1, \ldots, a_l) \equiv (a'_1, \ldots, a'_l)(\pi) \Leftrightarrow (\varphi_1(a_1, \ldots, a_l), \ldots, \varphi_m(a_1, \ldots, a_l)) = \\ = (\varphi_1(a'_1, \ldots, a'_l), \ldots, \varphi_m(a'_1, \ldots, a'_l)). \tag{33}$$

Определим отображение $\psi : \pi \to X$ следующим образом: $\psi(C) = b$ $(C \in \pi)$ тогда и только тогда, когда $(\varphi_1(a_1, \ldots, a_l), \ldots, \varphi_m(a_1, \ldots, a_l)) \in B_f(b)$ для некоторого (а в силу (33) для каждого) набора $(a_1, \ldots, a_l) \in C$. Положим $S(b) = \{C \in \pi \mid \psi(C) = b\}$ $(b \in X)$.

Из определения отображения ψ и множеств $S(b)$ $(b \in X)$ вытекает, что истинны равенства

$$B_g(b) = \bigcup_{C \in S(b)} C \quad (b \in X). \tag{34}$$

Исходя из равенств (32) и (34) получаем, что

$$\mathsf{P}_g(b) = \begin{cases} \dfrac{\sum_{C \in S(b)} |C|}{|X|^l}, & \text{если } b \in \operatorname{Val} f, \\ 0, & \text{если } b \notin \operatorname{Val} f. \end{cases}$$

Следовательно, отображение f и суперпозиция g статистически эквивалентны тогда и только тогда, когда существует такая подстановка $h : \operatorname{Val} f \to \operatorname{Val} f$, что истинны равенства

$$\frac{\sum_{C \in S(h(a))} |C|}{|X|^l} = \frac{|B_f(a)|}{|X|^m} \quad (a \in \operatorname{Val} f),$$

т.е. равенства

$$\sum_{C \in S(h(a))} |C| = |X|^{l-m} |B_f(a)| \quad (a \in \operatorname{Val} f). \tag{35}$$

Таким образом, равенства (35) представляют собой критерий статистической эквивалентности отображения $f \in \mathsf{F}_m(X)$ и суперпозиции $g \in \mathsf{F}_l(X)$ отображения f и набора отображений $\varphi_i \in \mathsf{F}_l(X)$ $(i = 1, \ldots, m)$ при условии, что $\operatorname{Val} g = \operatorname{Val} f$.

ЗАКЛЮЧЕНИЕ

В настоящей работе разработан фрагмент теории, предназначенной для исследования статистически эквивалентных отображений вида $f : X^l \to X$ $(l \in \mathbf{N})$, где X $(|X| \geq 2)$ — конечное множество. Решены основные модельные задачи: исследование коллизии отображений, анализ вычислительной стойкости последовательности отображений при неограниченном росте числа переменных и вычисление асимптотической вычислительной стойкости этой последовательности отображений, анализ структуры классов статистически эквивалентных отображений, исследование условия статистической эквивалентности отображения и суперпозиции этого отображения с заданным набором отображений.

Одним из направлений дальнейших исследований является обобщение и детальная отработка полученных результатов для векторных отображений вида $\mathbf{f} = (f_1, \ldots, f_n)$, где $f_i : X^l \to X$ $(l \in \mathbf{N})$ для всех $i = 1, \ldots, n$.

В работе приведено два примера множеств статистически эквивалентных отображений над конечными ассоциативно-коммутативными кольцами специального вида. Построение нетривиальных множеств статистически эквивалентных отображений над конечным ассоциативным кольцом специального вида (в частности, для матричного кольца над конечным полем) и решение для них перечисленных выше модельных задач представляют собой второе направление исследований.

При решении задач защиты информации часто используются рекуррентные последовательности вида $x_{n+l} = f(x_{n+l-1}, \ldots, x_n)$ $(n \in \mathbf{N})$, где $l \in \mathbf{N}$ — фиксированное число. Поэтому детальная обработка полученных результатов для рекуррентных последовательностей указанного вида актуальна с теоретической и прикладной точек зрения. Решение этой задачи представляет собой третье направление исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин и др. — М.: Гелиос АРВ, 2002. — 480 с.
2. Зубов А.Ю. Совершенные шифры. — М.: Гелиос АРВ, 2003. — 160 с.
3. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев и др. — Минск: Новое знание, 2003. — 382 с.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. — М.: ТРИУМФ, 2003. — 816 с.
5. Скобелев В.В., Скобелев В.Г. Анализ шифрсистем. — Донецк: ИПММ НАН Украины, 2009. — 479 с.
6. Скобелев В.В. Моделирование автоматов над кольцом автоматами с конечной памятью // Проблемы управления и информатики. — 2012. — № 3. — С. 114–122.
7. Скобелев В.В., Скобелев В.Г. О сложности анализа автоматов над конечным кольцом // Кибернетика и системный анализ. — 2010. — № 4. — С. 17–30.
8. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979. — 536 с.
9. Горицкий В.М. Вероятностная криптография в системах защиты информации: кодовая защита // Электроника и связь. — 1998. — Вып. 5. — С. 140–145.
10. Скобелев В.В. Анализ семейств хэш-функций, определяемых автоматами над конечным кольцом // Кибернетика и системный анализ. — 2013. — № 2. — С. 46–55.
11. Шеннон К.Э. Теория связи в секретных системах // Работы по теории информации и кибернетики. — М.: ИЛ, 1963. — С. 333–402.
12. Буй Д.Б., Богатирьова Ю.О. Сучасний стан теорії мультимножин // Вісн. Київ. нац. ун-ту імені Тараса Шевченка. Сер.: фіз.-мат. науки. — 2010. — Вип. 1. — С. 51–58.

Поступила 16.01.2014