

$H, ZH > H, M, P : 0,05 \frac{H \cdot ZH}{N}$: раствор (хищник должен найти и убить жертву, и будет пища);

$H, P > 2H : 0,05 \frac{H \cdot P}{N}$: смесь (хищники находят принесённую пищу и размножаются).

На рис. 1 показаны результаты реализации этой модели программой «Популяция». Моделирование обходится без получения системы нелинейных дифференциальных уравнений динамики средних.

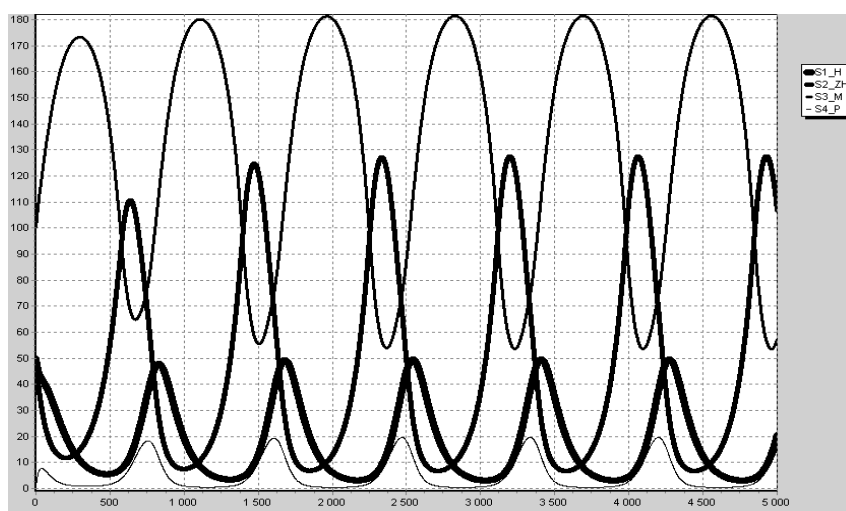


Рис. 1. Хищники и жертвы в ограниченной экологической нише.

H — количество хищников; ZH — количество жертв; M — количество экологических мест; P — количество добытой пищи

Следует заметить, что в предлагаемой программе моделирования вовсе не обязательно подробно описывать вероятности переходов, заданные здесь формулами. Достаточно задать только численные характеристики — коэффициенты модели (здесь 0,01 и 0,05) и типы нелинейных переходов. Остальные части вероятностей переходов ($\min\{ZH, M\}$ и $H \cdot ZH/N$) стандартны и вычисляются программой согласно типу перехода.

ЛИТЕРАТУРА

1. Воробьев В. А., Кочнев А. И. Популяционное моделирование коллективного поведения автоматов // Вестник Томского государственного университета. Приложение. 2007. № 23. С. 270–275.
2. Ачасова С. М., Бандман О. Л. Корректность параллельных вычислительных процессов. Новосибирск: Наука, 1990. 314 с.

УДК 512.5

О СКЕЛЕТНЫХ АВТОМАТАХ

В. Н. Салий

Под автоматом понимается тройка $A = (S, X, \delta)$, где S и X — конечные непустые множества (состояний и входных сигналов соответственно); $\delta : S \times X \rightarrow S$ — отображение, называемое функцией переходов. Функция переходов продолжается на множество $S \times X^*$, где X^* — совокупность всех конечных слов над алфавитом X : по опре-

делению, $\delta(s, e) = s$ для любого $s \in S$ и пустого слова e и $\delta(s, px) = \delta(\delta(s, p), x)$ для любых $s \in S$, $x \in X$, $p \in X^*$.

Автомату A сопоставляется диаграмма переходов — мультиграф $G(A)$, вершинами которого являются элементы множества S и дуги помечены элементами из X : из вершины s в вершину s' ведет дуга с меткой x , если $\delta(s, x) = s'$.

Говорят, что состояние s' достижимо в автомате A из состояния s , если существует входное слово $p \in X^*$, такое, что $\delta(s, p) = s'$. В этом случае пишут $(s, s') \in \tau$, и так определенное отношение $\tau \subseteq S \times S$ называют отношением достижимости в автомате A . Его симметричная часть $\sigma = \tau \cap \tau^{-1}$ называется отношением взаимной достижимости в автомате A . Классы эквивалентности σ называют слоями автомата A . В [1] введено понятие каркаса автомата. Каркас автомата A — это упорядоченное множество $(F(A), \leq)$, элементами которого являются слои автомата A , а порядком на множестве слоев $F(A) = A/\sigma$ — отношение, обратное отношению достижимости τ . Очевидно, что для любого автомата A выполняются неравенства $1 \leq |F(A)| \leq |S|$. Если $|F(A)| = 1$, т. е. отношение σ универсально, автомат A называется сильносвязным. Если же $|F(A)| = |S|$, т. е. отношение σ тождественно, $\sigma = \Delta$, автомат A назовем скелетным. В скелетном автомате отношение достижимости τ является порядком на множестве состояний S .

Поскольку в скелетном автомате A все слои одноэлементны, можно считать, что в этом случае каркасом является множество S , упорядоченное обратной достижимостью τ^{-1} , так что $s \geq s'$ означает, что состояние s' достижимо из состояния s .

Нумерацией состояний автомата называется биективное отображение множества его состояний S на начальный отрезок $[1, m]$ натурального ряда. Нумерация, по определению, является правильной, если состояния, достижимые из данного состояния, имеют меньшие, чем у него, номера.

Теорема 1. В автомате A существует правильная нумерация состояний тогда и только тогда, когда A — скелетный автомат.

Подмножество $S' \subseteq S$ называется устойчивым в автомате A , если $\delta(s, x) \in S'$ для любых $s \in S'$ и $x \in X$. Если S' устойчиво в A , то, ограничивая функцию переходов δ на $S' \times X$, получают подавтомат $A' = (S', X, \delta)$. Совокупность $\text{Sub}A$ всех подавтоматов автомата A , упорядоченная отношением $A_1 \leq A_2 \iff S_1 \subseteq S_2$, где $A_i = (S_i, X, \delta)$, $i = 1, 2$, является дистрибутивной решеткой. Это решетка подавтоматов автомата A .

Известно [2], что для каждого автомата A существует автомат B с двумя входными сигналами, такой, что $\text{Sub}A \cong \text{Sub}B$, и что не всегда найдется автономный (т. е. с $|X| = 1$) автомат B с такой же, как у A , решеткой подавтоматов. Минимизацию по числу состояний дает следующее предложение.

Теорема 2. Пусть $A = (S, X, \delta)$ и $B = (T, Y, \gamma)$ — автоматы, такие, что $\text{Sub}A \cong \text{Sub}B$. Тогда $|T| \geq |F(A)|$. При этом существует скелетный автомат B , такой, что $\text{Sub}A \cong \text{Sub}B$ и $|T| = |F(A)|$.

Пусть K — некоторый класс автоматов и $A \notin K$. Как можно путем в том или ином смысле минимальных изменений в структуре автомата A получить из него автомат A' из класса K ? В числе допустимых приемов реконструкции автомата можно рассматривать, например, отождествление некоторых вершин (факторизация), введение дополнительных состояний и/или входных сигналов (расширения), перенаправление дуг диаграммы переходов, удаление дуг (замена их петлями) и т. п.

Показано, как путем удаления минимального числа дуг в диаграмме переходов $G(A)$ можно получить из данного автомата A скелетный автомат.

Подробное изложение представленных результатов можно найти в [3].

ЛИТЕРАТУРА

1. Салий В. Н. Каркас автомата // Прикладная дискретная математика. 2010. № 1(7). С. 63–67.
2. Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем. М.: Наука, 1997. 368 с.
3. Салий В. Н. Скелетные автоматы // Прикладная дискретная математика. 2011. № 2(12). С. 73–76.

УДК 004.056.55

АТАКА АППАРАТНОГО СБОЯ НА РЕАЛИЗАЦИЮ ШИФРА ЗАКРЕВСКОГО НА ОСНОВЕ ПЕРЕСТРАИВАЕМОГО АВТОМАТА¹

В. Н. Тренькаев

В последние годы растет количество криптографических атак, использующих особенности реализации, так называемые атаки по побочным каналам (side channel attacks) [1], которые часто дают более мощный результат, чем классический криптоанализ. Рассматривается вариант такой атаки — атака на основе сбоев (fault attack), когда криптоаналитик имеет возможность оказать на шифратор внешнее физическое воздействие и вызвать ошибки (сбои) в процессе его работы. Предложена атака аппаратного сбоя на реализацию шифра Закревского на базе перестраиваемого автомата [2]. Предполагается, что нештатные условия получаются созданием кратковременной ошибки в процессе работы шифратора в виде фиксирования требуемого значения одного бита. Криптоанализ шифра Закревского как автоматного шифра сводится к построению простого условного эксперимента по восстановлению (идентификации) автомата из заданного класса.

Конечный автомат задаётся пятеркой (X, S, Y, ψ, φ) , где S — конечное непустое множество состояний; X и Y — конечные входной и выходной алфавиты соответственно, причем $|X| = |Y|$; $\psi : X \times S \rightarrow S$ и $\varphi : X \times S \rightarrow Y$ — функции переходов и выходов соответственно.

Под перестраиваемым понимается автомат с возможностью выбора функции переходов из заданного множества. Структура перестраиваемого автомата, на базе которого реализуется шифр Закревского, представлена на рис. 1, где компоненты ψ_0 и ψ_1 реализуют функции $\psi_0 : X \times S \rightarrow S$ и $\psi_1 : X \times S \rightarrow S$ соответственно. Компонента Key реализует функцию $C : X \times S \times K \rightarrow \{0, 1\}$, где K — конечное множество настроек. На схеме представлен также мультиплексор Mux, который в зависимости от значения функции $C_k(x, s) = C(x, s, k)$ осуществляет выбор одного из двух возможных состояний $\psi_0(x, s)$ и $\psi_1(x, s)$, «пропуская» его далее в регистр памяти Reg, где в каждый момент автоматного времени хранится текущее состояние. Компонента Out реализует функцию выходов $\varphi(x, s)$, такую, что при любом $s \in S$ функция $\varphi_s(x) = \varphi(x, s)$ является биекцией из X в Y и все биекции $\varphi_s(x)$, $s \in S$, различные. Каждой настройке $k \in K$ перестраиваемого автомата соответствует автомат Закревского $Z^{(k)} = (X, S, Y, \psi^{(k)}, \varphi)$, у которого $\psi^{(k)}(x, s) = \psi_c(x, s)$ для всех $(x, s) \in X \times S$ и $c = C_k(x, s)$. Функции ψ_0 и ψ_1 устроены так [2], что автомат $Z^{(k)}$ сильносвязный. Автомат $Z^{(k)^{-1}} = (Y, S, X, \psi^{(k)}, \varphi')$,

¹Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).