избежать потери полноты базовым алгоритмом решения SAT-задачи (данный негативный эффект, возникающий в современных SAT-решателях, был отмечен в [4]). Предполагается рассмотреть результаты вычислительных экспериментов по использованию гибридного подхода (SAT+ROBDD) в распределенных вычислительных средах.

ЛИТЕРАТУРА

1. *Семенов А. А., Заикин О. С., Беспалов Д. В. и др.* Решение задач обращения дискретных функций на многопроцессорных вычислительных системах // Труды Четвертой Междунар. конф. «Параллельные вычисления и задачи управления» PACO'2008, Москва, 26–29 октября 2008. 2008. С. 152–176.
2. *Семенов А. А., Заикин О. С., Беспалов Д. В., Ушаков А. А.* SAT-подход в криптоанализе некоторых систем поточного шифрования // Вычислительные технологии. 2008. Т. 13. № 6. С. 134–150.
3. *Заикин О. С., Семенов А. А.* Технология крупноблочного параллелизма в SAT-задачах // Проблемы управления. 2008. № 1. С. 43–50.
4. *Семенов А. А., Заикин О. С.* Неполные алгоритмы в крупноблочном параллелизме комбинаторных задач // Вычислительные методы и программирование. 2008. Т. 9. № 1. С. 112–122.

УДК 681.3+519.71

ОБОБЩЕННАЯ ОБРАТИМОСТЬ ДИНАМИЧЕСКИХ СИСТЕМ В ЗАДАЧАХ ШИФРОВАНИЯ

А. М. Ковалев, В. А. Козловский, В. Ф. Щербак

Рассматривается метод преобразования оцифрованной информации, основанный на дискретной динамической системе, порождающей передаточное отображение: вход (информационное сообщение) — выход (закодированное сообщение). Восстановление входа осуществляется с помощью специальным образом построенной обратной системы. Предложены конструкции обратимых систем, обладающие различной степенью обратимости: обратимые, идентифицируемые и обратимые на множестве траекторий. Рассмотрены конечно-автоматные конструкции, реализующие указанный подход.

Пусть передача информации осуществляется с помощью дискретной динамической системы, правые части которой зависят от вектор-функции $u(.)$ — оцифрованного информационного сообщения:

$$x(k+1) = f(x(k), u(k)), \quad x(0) = x_0, \tag{1}$$

$$y(k) = h(x(k), u(k)), \quad y \in R^m, \tag{2}$$

где $x(.) \in R^n$, $u(.) \in R^m$, $y(.) \in R^m$ определяют векторы состояния системы, ее вход и выход соответственно. По каналам связи передается выходной сигнал — функция $y(k)$, зависящая от состояния системы, ее параметров и сообщения $u(k)$. Рассматривается задача восстановления значений входного воздействия по значениям функции выхода. В теории управления непрерывными динамическими системами одним из способов ее решения является построение системы, обратной к исходной [1, 2]. Базовым свойством таких систем является обратимость. В терминах теории управления динамические системы, пригодные для преобразования и передачи информации, составляют класс обратимых систем управления. При этом многомерность динамической системы, наличие сложных взаимосвязей между переменными позволяют конструировать системы

разного уровня сложности, требущие для восстановления неизвестного входа дополнительную информацию разного рода. Рассмотрены конструкции таких систем, обладающих различной степенью обратимости: идентифицируемые, обратимые, обратимые на нескольких траекториях. Показано, что при использовании множества траекторий максимально широкий класс динамических система становится идентифицируемым. Предлагается соответствующая схема передачи и восстановления сообщения, в которой передаваемый сигнал используется для синтеза дополнительных выходов системы, после чего восстановление входа системы осуществляется с использованием сигнала, заданного на множестве траекторий.

При реализации таких систем на компьютере, например, как криптографических систем, возникает необходимость перехода к дискретным аналогам непрерывных динамических систем. Такие аналоги предложены в виде конечных автоматов, описываемых системами уравнений над конечными полями или кольцами. При этом разные типы обратимости получают естественную теоретико-автоматную интерпретацию. Введено понятие k-кратного без потери информации автомата (k-БПИ), которое аналогично понятию обратимости на нескольких траекториях. Для ряда систем (Лоренца, Рёсслера, Чуа) введены их автоматные аналоги и на их основе предложены поточные криптоалгоритмы. В рамках теории экспериментов с автоматами выполнена формализация атак на такие криптосистемы и доказана NP-полнота задачи о распознавании контрольного эксперимента для k-БПИ-автоматов, лежащая в основе такой формализации.

Использование методики нескольких траекторий для обратимых нелинейных динамических систем и их автоматных аналогов, задаваемых уравнениями над конечными кольцами и полями, позволяет разработать метод управления размерностью пространства состояний, отличный от метода, предложенного в работе [3]. При этом возникает система с переменной структурой, в которой к ключевым параметрам (элементам кольца или поля) добавляется структурный ключ, с помощью которого осуществляется выбор количества траекторий передающей системы.

ЛИТЕРАТУРА

1. *Ковалев А. М., Щербак В. Ф.* Управляемость, наблюдаемость, идентифицируемость динамических систем. Киев: Наук. думка, 1993. 285 с.
2. *Feldmann U., Hasler M., Schwarz W.* Communication by chaotic signals: the inverse system approach // Int. J. Circ. Theory Appl. 1996. V. 24. P. 551–579.
3. *Ковалев А. М., Козловский В. А., Щербак В. Ф.* Обратимые динамические системы с переменной размерностью фазового пространства в задачах криптографического преобразования информации // Прикладная дискретная математика. 2008. № 2(2). С. 39–44.

УДК 519.7

О ПОТОЧНЫХ И АВТОМАТНЫХ ШИФРСИСТЕМАХ

И. В. Панкратов

Ранее в работе автора [1] были определены понятия поточной шифрсистемы и самосинхронизирующихся с задержкой поточной и регистровой шифрсистем и было показано, что последними исчерпываются все поточные самосинхронизирующиеся системы, у которых проекции генератора ключевого потока являются сильносвязными автоматами. В настоящей работе определяются ещё и понятия автоматной и самосинхронизирующейся с задержкой автоматной шифрсистем и устанавливается, что реги-