УДК 519.713

ЭКСПЕРИМЕНТЫ ПО ВОССТАНОВЛЕНИЮ ПЕРЕХОДОВ АВТОМАТА С БИЕКТИВНОЙ ФУНКЦИЕЙ ВЫХОДОВ

В. Н. Тренькаев

Конечный автомат называется автоматом с биективной функцией выходов (автоматом без потери информации по [1]), если при фиксации любого состояния такой автомат осуществляет взаимно однозначное отображение множества входных символов на множество выходных символов. Известно [2], что автоматы данного класса используются в криптографии для шифрования конфиденциальной информации. Шифрующий автомат преобразует осмысленные открытые тексты в нечитаемые шифрованные. При этом существует возможность однозначно восстановить исходный открытый текст по известному шифрованному тексту и ключу. Обычно в качестве ключа берется начальное состояние шифрующего автомата. «Засекречивание» подмножества переходов автомата может существенно повысить способность таких автоматных шифров противостоять различным атакам.

При адаптивной атаке с выбранным открытым текстом считается, что криптоаналитик имеет возможность подавать на шифратор специально подобранные открытые тексты и наблюдать соответствующие шифрованные тексты. Таким образом, в рамках автоматной модели мы имеем задачу восстановления подмножества переходов автомата с помощью проведения простого условного эксперимента. Причем будем считать, что эксперимент может иметь неопределенный исход, т. е. нет гарантии того, что в результате будут распознаны все секретные переходы. Это соответствует ситуации, когда мы имеем метод криптоанализа с надежностью (вероятностью дешифрования [2]), не равной единице. Использование простых условных экспериментов предполагает, что у экспериментатора имеется в наличии только один экземпляр автомата-шифратора и по ходу эксперимента возможно изменение предъявляемых автомату входных слов в зависимости от его выходных реакций на предъявленные ранее слова.

Конечным автоматом A называется пятерка (S, X, Y, ψ, φ), где S — конечное непустое множество состояний, X и Y — конечные входной и выходной алфавиты соответственно, причем $|X| = |Y|$, а $\psi : S \times X \to S$ и $\varphi : S \times X \to Y$ — функции переходов и выходов соответственно. Четверка $s - x/y \to s'$, где $s' = \psi(s, x)$ и $y = \varphi(s, x)$, есть переход автомата A. Состояние s' называется преемником состояния s по символу x. Автомат A есть автомат с биективной функцией выходов, если для любого $s \in S$ функция $\varphi_s(x) = \varphi(s, x)$ определяет взаимно однозначное отображение X на Y. Автомат A является сильносвязным, если из любого состояния $s \in S$ достижимо любое другое состояние $s' \in S$, т. е. существует последовательность переходов $s = s_1 - x_1/y_1 \to s_2, s_2 - x_2/y_2 \to s_3, \ldots, s_k - x_k/y_k \to s_{k+1} = s'$. В этом случае говорят, что слово $x_1 x_2 \ldots x_k$ переводит автомат A из состояния s в состояние s'. Установочным называется входное слово, наблюдая реакцию на которое, можно определить текущее состояние автомата. Следуя [3], будем называть начальным идентификатором состояния s множество пар x/y, где x — входной символ, а $y = \varphi_s(x)$, которое однозначно характеризует состояние s, т. е. начальные идентификаторы любых различных состояний различны.

Постановка задачи. Для эксперимента предъявлен сильносвязный автомат A с биективной функцией выходов, часть переходов которого неизвестна. Среди $\varphi_s(x), s \in S$, не существует равных функций, а также для любого $s \in S$ существует не более одного

неизвестного перехода $s - x/y \to p$. Требуется путем проведения простого условного эксперимента с автоматом A определить неизвестные (секретные) переходы.

Восстановление функции выходов. Пусть для $a \in X$ значение функции $\varphi_s(a)$ неизвестно. Поскольку функция φ_s есть биекция, то образ символа a относительно φ_s вычисляется как разность множеств Y и $\{y : y = \varphi_s(x), x \in X \backslash \{a\}\}$.

Восстановление функции переходов. Отметим, что начальный идентификатор для любого состояния s автомата, предъявленного для эксперимента (после восстановления функции выходов), может быть построен как $id(s) = \{x/y : x \in X, y = \varphi_s(x)\}$.

Шаг 1. $L := S$, т. е. автомат A может находиться в любом из своих состояний.

Шаг 2 (построение установочного слова). Найти входной символ x, такой, что существуют два состояния s и s' из L, для которых $\varphi(s, x) \neq \varphi(s', x)$. Подать на автомат A входной символ x и пронаблюдать выходной символ y. Найти состояния из L, стартуя из которых автомат A может выдавать y, т. е. построить множество $N = \{s : s \in L, y = \varphi_s(x)\}$. Построить множество Q преемников состояний из N по символу x. Если существует $s \in N$, соответствующее начальному состоянию секретного перехода $s - x/y \to p$, то перейти на Шаг 1. Если $|Q| \neq 1$, то $L := Q$ и перейти на Шаг 2.

Шаг 3 (построение переводящего слова). Найти и подать на A входное слово, переводящее автомат из состояния $q \in Q$, причем $|Q| = 1$, в неизвестное состояние k, соответствующее финальному состоянию секретного перехода $s - x/y \to p$.

Шаг 4 (восстановление неизвестного состояния). На автомат A подать входной символ a и пронаблюдать выходной символ b. $ID_k := ID_k \cup a/b$. Если $|ID_k| = |X|$, то состояние $k := p$, где p такое, что $id(p) = ID_k$, т. е. переход $s - x/y \to p$ восстановлен. Если существуют невосстановленные переходы, то перейти на Шаг 1.

ЛИТЕРАТУРА

1. *Кудрявцев В. Б., Алешин С. В., Подколзин А. С.* Введение в теорию автоматов. М.: Наука, 1985. 320 с.
2. *Бабаш А. В., Шанкин Г. Н.* Криптография. М.: СОЛОН-Р, 2002. 512 с.
3. *Грунский И. С., Козловский В. А.* Синтез и идентификация автоматов. Киев: Наукова думка, 2004. 245 с.

УДК 519.725; 519.816; 519.712.6

ПРОТОКОЛ АРГУМЕНТА ЗНАНИЯ СЛОВА КОДА ГОППЫ И ОШИБКИ ОГРАНИЧЕННОГО ВЕСА

В. Е. Федюкович

Рассматривается задача проверки утверждения об ошибке в искаженном кодовом слове кода Гоппы. Дополнительным условием является предоставление проверяющей стороне минимально необходимой информации о структуре кода, кодовом слове и весе ошибки. Рассматриваются интерактивные протоколы (interactive proof system) и протоколы доказательства знания (proof of knowledge) значений, из которых получены экземпляры привязки (commitment). Произвольный Доказывающий, который не знает компонентов кодового слова и коэффициентов полинома Гоппы, удовлетворяющих проверяемым условиям, имеет только ничтожную вероятность успешно завершить протокол с честным Проверяющим.

Рассматриваются протоколы аргумента, в которых как Проверяющий, так и Доказывающий располагают только полиномиальными ресурсами. Рассматривается схема