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 АВТОМАТА[1]

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 $|X| = |Y|$; $\psi : X \times S \to S$ и $\varphi : X \times S \to Y$ — 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 $\psi_0 : X \times S \to S$ и $\psi_1 : X \times S \to S$ соответственно. Компонента Key реализует функцию $C : X \times S \times K \to \{0, 1\}$, 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 $Z^{(k)^{-1}} = (Y, S, X, \psi^{(k)}, \varphi')$,

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

где $\varphi'(y, s) = x$, если $\varphi(x, s) = y$, обратен автомату $Z^{(k)}$. В одном и том же начальном состоянии s_0 автоматы $Z^{(k)}$ и $Z^{(k)^{-1}}$ представляют собой алгоритмы соответственно шифрования и расшифрования на ключе $(k, s_0) \in K \times S$ и в совокупности образуют то, что называется шифром Закревского.

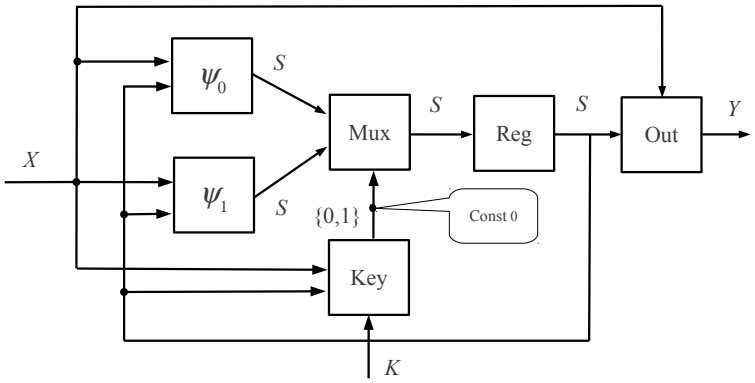

Рис. 1. Структура перестраиваемого автомата

Предполагается, что криптоаналитику о перестраиваемом автомате известно всё, кроме настройки $k \in K$ и начального состояния s_0 — состояния регистра Reg. В этом случае функция $\psi^{(k)}$ определяется однозначно настройкой k. Вместе с тем $\psi^{(k)}$ и s_0 однозначно определяют алгоритмы шифрования и расшифрования, поэтому атаку с угрозой раскрытия пары $(\psi^{(k)}, s_0)$ можно считать атакой с угрозой раскрытия алгоритма шифрования (расшифрования). Именно такой является описываемая далее атака аппаратного сбоя на шифр Закревского, реализуемый перестраиваемым автоматом на рис. 1.

Сначала для автомата $A_0 = (X, S, Y, \psi_0, \varphi)$ строится установочное слово α, т. е. входное слово, наблюдая реакцию на которое, можно однозначно определить текущее состояние автомата. Далее производится воздействие на шифратор, такое, что выход компонеты Key имеет фиксированное значение 0 (Const 0 на рис. 1). Затем на шифратор подается установочное слово α и по реакции на него определяется текущее состояние шифратора. После этого опять производится воздействие на шифратор, которое снимает фиксацию выхода компоненты Key. Наконец, проводится простой условный эксперимент по восстановлению автомата $Z^{(k)}$, который сводится к процедуре определения неизвестного $s' = \psi^{(k)}(x, s)$ при известном s и неизвестном $\psi^{(k)}$. По свойствам перестраиваемого автомата $s' \in \{\psi_0(x, s), \psi_1(x, s)\}$ и существует хотя бы один входной символ z, такой, что $\varphi(z, \psi_0(x, s)) \neq \varphi(z, \psi_1(x, s))$. Тогда по реакции автомата $Z^{(k)}$ на входное слово xz можно однозначно идентифицировать состояние s'. Эта операция проделывается до тех пор, пока возможно, после чего строится входное слово, переводящее автомат $Z^{(k)}$ в известное начальное состояние некоторого нераспознанного перехода, и операция повторяется. Процесс заканчивается с определением $\psi^{(k)}(x, s)$ для всех $(x, s) \in X \times S$.

ЛИТЕРАТУРА

1. *Панасенко С. П.* Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. 576 с.
2. *Тренькаев В. Н.* Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.