крипт
УДК 519.7 DOI 10.17223/2226308X/12/26

О КРИПТОАНАЛИТИЧЕСКОЙ ОБРАТИМОСТИ С КОНЕЧНОЙ ЗАДЕРЖКОЙ КОНЕЧНЫХ АВТОМАТОВ

Г. П. Агибалов

Рассматривается свойство обратимости с конечной задержкой конечных автоматов с позиции криптоаналитика, а именно в зависимости от априорной информации, доступной алгоритму обращения. В криптоанализе, например симметричных конечно-автоматных шифров атакой с известным шифртекстом, типична ситуация, когда задачу обращения автомата приходится решать частично осведомлённому криптоаналитику. В зависимости от этой осведомлённости можно определить 208 различных типов обратимости и обратимых автоматов, изучить их свойства и установить соотношения между ними. Общеизвестные понятия сильной и слабой обратимости автоматов — это только два из этих типов. Целью настоящего доклада является обсуждение понятия криптоаналитической обратимости автоматов. Назван ряд математических задач (от характеризации автоматов, криптоаналитически обратимых разного типа, до создания на их основе криптосистем с открытым и закрытым ключом и их криптоанализа), которые представляют собой интересный предмет для дальнейших исследований и публикаций.

Ключевые слова: *конечные автоматы, автоматы без потери информации, обратимость автоматов, криптоаналитическая обратимость.*

Предлагаемые вниманию тезисы доклада являются расширенным рефератом работы автора [1], содержащей определение обратимости с конечной задержкой конечных автоматов с криптоаналитической точки зрения, по которой обращение автоматного преобразования осуществляется с целью восстановления входного слова автомата по его выходной последовательности при наличии некоторой частичной информации об этом преобразовании. Разные типы этой информации определяют разные типы и классы криптоаналитической обратимости автоматов и порождают многочисленные теоретико-автоматные и криптографические задачи, требующие математического решения. Обширный список этих задач включает в себя такие задачи, как, например, установление необходимых и достаточных условий автоматной обратимости каждого типа, построение конструктивных тестов принадлежности автоматов конкретным классам обратимости, алгоритмический синтез автоматов в заданных классах обратимости, характеризация обратимых автоматов, допускающих обратные автоматы, алгоритмический синтез обратных автоматов каждого типа, разработка эффективных алгоритмов восстановления входных последовательностей обратимых автоматов в конкретных классах обратимости, создание криптосистем с закрытым и открытым ключами на базе обратимых автоматов определённых классов обратимости, алгоритмический криптоанализ таких криптосистем с оценками его вычислительной сложности.

Произвольный конечный автомат представляется как $A = (X, Q, Y, \psi, \varphi)$, где X, Q и Y суть его входной алфавит, множество состояний и выходной алфавит соответственно; ψ и φ — его функции соответственно переходов и выходов, $\psi : X \times Q \to Q$ и $\varphi : X \times Q \to Y$. Последние, будучи определёнными для пар $xq \in X \times Q$, распространяются на пары $\alpha q \in X^* \times Q$ индукцией по длине $|\alpha|$ слова $\alpha \in X^*$, а именно определяются функции $\psi : X^* \times Q \to Q$ и $\bar{\varphi} : X^* \times Q \to Y^*$ как $\psi(\Lambda, q) = q$, $\psi(\alpha\beta, q) = \psi(\beta, \psi(\alpha, q))$,

$\bar{\varphi}(\Lambda, q) = \Lambda$, $\bar{\varphi}(x, q) = \varphi(x, q)$ и $\bar{\varphi}(\alpha\beta, q) = \bar{\varphi}(\alpha, q)\bar{\varphi}(\beta, \psi(\alpha, q))$. Символ Λ здесь обозначает пустое слово в любом алфавите.

Таким образом, $\psi(\alpha, q)$ — это состояние, в которое автомат A переходит из состояния q под действием входного слова α, а $\bar{\varphi}(\alpha, q)$ — это выходное слово, которое он при этом выдает.

Наконец, всюду далее под τ подразумевается произвольное целое неотрицательное число, называемое задержкой, и в отсутствие дополнительных оговорок в записи логических формул предполагается, что $a \in X$, $b \in X$, $\alpha \in X^*$, $\beta \in X^*$, $\delta \in X^\tau$, $\varepsilon \in X^\tau$, $q \in Q$, $s \in Q$.

Рассмотрим произвольный конечный автомат $A = (X, Q, Y, \psi, \varphi)$. Пусть q, α, δ — переменные со значениями в Q, X^*, X^τ, обозначающими соответственно начальное состояние, префикс (начало) и суффикс (окончание) входного слова $\alpha\delta$ автомата A, и $K = \{\forall q, \forall\alpha, \forall\delta, \exists q, \exists\delta\}$ — множество кванторов общности и существования по этим переменным. Заметим, что в K нет квантора $\exists\alpha$. Это связано с тем, что для криптоаналитика префикс α входного слова автомата предполагается неизвестным и не некоторым, но любым. Пусть также $\theta = \psi(\alpha, q)$, $t = \psi(\alpha\delta, q)$ и $V = \{\Lambda, q, \theta, t, \delta, q\theta, qt, q\delta, \theta t, \theta\delta, t\delta, q\theta t, q\theta\delta, qt\delta, \theta t\delta, q\theta t\delta\}$. Символами θ и t обозначены, как видно, промежуточное и заключительное состояния, в которые автомат A переходит из состояния q под действием входных слов α и $\alpha\delta$ соответственно. Элементы множества V предназначены для задания того, что называется здесь порядком обратимости автомата A. Они являются по существу функциями от q, α, δ.

Мы говорим, что автомат A *обратим с задержкой* τ, если существуют кванторы K_1, K_2, K_3 в K с разными переменными из $\{q, \alpha, \delta\}$, а также функция $f : Y^* \times V \to X^*$ и элемент $\upsilon(q, \alpha, \delta) \in V$, такие, что истинна формула

$$F = K_1K_2K_3(f(\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) = \alpha);$$

в этом случае $(K_1K_2K_3, \upsilon)$ называется *типом обратимости* автомата A, $K_1K_2K_3$ — *степенью обратимости*, υ — *порядком обратимости*, f — *функцией восстановления* (входного префикса), τ — *задержкой восстановления*, или *обратимости* и выражение $\exists f[F]$ — *условием обратимости* данного типа автомата A. Тип обратимости, в котором все кванторы являются кванторами общности, называется впредь *универсальным*.

В определении обратимого автомата степень обратимости $(K_1K_2K_3)$ своими кванторами $(\forall, \exists)$ указывает на степень полноты областей используемых (всех или некоторых) значений переменных q, α, δ, а их последовательностью — на зависимость значений одних (последующих) переменных от других (предшествующих). Порядок обратимости в нём содержит дополнительную информацию, известную криптоаналитику априорно. Это может быть и начальное состояние q автомата, и его промежуточное состояние $\theta = \psi(\alpha, q)$, и заключительное состояние $t = \psi(\alpha\delta, q)$, и суффикс δ входного слова.

Степень обратимости $(K_1K_2K_3)$ может принимать тринадцать различных значений, а порядок обратимости υ — шестнадцать значений, поэтому количество всех типов обратимости $(K_1K_2K_3, \upsilon)$ с фиксированной задержкой автомата A равно 208. Два из них, а именно (сильная) обратимость и слабая обратимость, хорошо известные и в теории автоматов и в криптографии [2, 3], в нашей теории универсальные и представлены наборами $(\forall q\forall\alpha\forall\delta, \varnothing)$ и $(\forall q\forall\alpha\forall\delta, \{q\})$, обозначающими произвольность (полноту областей) значений переменных q, α, δ, а также отсутствие у криптоаналитика дополнительной информации и известность ему начального состояния автомата

соответственно. Условия обратимости этих двух типов выглядят следующим образом: $\exists f \forall q \forall \alpha \forall \delta (f(\bar{\varphi}(\alpha\delta, q)) = \alpha)$ и $\exists f \forall q \forall \alpha \forall \delta (f(\bar{\varphi}(\alpha\delta, q), q) = \alpha)$.

Пример ещё одного типа обратимости автомата A содержится в условии

$$\exists f \forall \alpha \exists \delta \forall q (f(\bar{\varphi}(\alpha\delta, q), q, \psi(\alpha\delta, q), \delta) = \alpha).$$

Это есть условие обратимости степени $\forall\alpha\exists\delta\forall q$ и порядка $\upsilon(q, \alpha, \delta) = (q, \psi(\alpha\delta, q), \delta)$. В нём утверждается возможность восстановления функцией f префикса α входного слова $\alpha\delta$ автомата по его выходному слову $\bar{\varphi}(\alpha\delta, q)$ при известных начальном состоянии q, заключительном состоянии $t = \psi(\alpha\delta, q)$ и суффиксе δ входного слова в предположении, что в автомате для каждого префикса α входного слова суффикс δ этого слова не любой, но свой, и для этого входного слова $\alpha\delta$ начальное состояние q может быть любым.

Каждому типу обратимости с фиксированной задержкой ставится в соответствие класс автоматов, обратимых этого типа. Показано, что граф отношения включения между этими классами представляет собой объединение двадцати девяти решёток, где каждая решётка по определению есть частично упорядоченное множество с точными верхней и нижней гранями для каждой пары его элементов. Доказано, что автомат A обратим типа $(\forall q \forall \alpha \forall \delta, \upsilon(q, \alpha, \delta))$, если и только если

$$\forall q \forall \alpha \forall \delta \forall s \forall \beta \forall \varepsilon (\alpha \neq \beta \Rightarrow (\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) \neq (\bar{\varphi}(\beta\varepsilon, s), \upsilon(s, \beta, \varepsilon)),$$

и что для любых символов кванторов $Q_i \in \{\forall, \exists\}$, $i \in \{1, 2, 3\}$, если автомат A обратим типа $(Q_1 x_1 Q_2 x_2 Q_3 x_3, \upsilon(q, \alpha, \delta))$, то

$$Q_1 x_1 Q_2 x_2 Q_3 x_3 Q_1 y_1 Q_2 y_2 Q_3 y_3 (\alpha \neq \beta \Rightarrow (\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) \neq (\bar{\varphi}(\beta\varepsilon, s), \upsilon(s, \beta, \varepsilon)),$$

где x_1, x_2, x_3 и y_1, y_2, y_3 — различные переменные из множеств $\{q, \alpha, \delta\}$ и $\{s, \beta, \varepsilon\}$ соответственно, такие, что если x_i есть q, α или δ, то y_i есть s, β или ε соответственно, и если $x_i = \alpha$, то $Q_i = \forall$.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Cryptanalytic concept of finite automaton invertibility with finite delay // Прикладная дискретная математика. 2019. № 44. С. 34–42.
2. *Агибалов Г. П.* Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 43–73.
3. *Tao R.* Finite Automata and Application to Cryptography. N.Y.: Springer, 2009. 406 p.

УДК 519.7 DOI 10.17223/2226308X/12/27

О ВЕРОЯТНОСТЯХ РАЗНОСТНЫХ ТРАЕКТОРИЙ SPONGE-ФУНКЦИИ BASH-F

С. В. Агиевич, А. С. Маслов, Ю. С. Ярошеня

Предлагаются два метода оценки снизу весов разностных траекторий sponge-функции Bash-f. Оценки ограничивают сверху вероятности траекторий и могут использоваться при обосновании стойкости основанных на Bash-f криптографических алгоритмов к разностным атакам. Для полных 24-тактовых траекторий лучшая из оценок ограничивает вероятности величиной 2^{-386}.

Ключевые слова: *sponge-функция, S-блок, разностный криптоанализ, разностная траектория.*