Бабаш Александр Владимирович, НИУ ВШЭ, 8 910 429 10 44, babash@yandex.ru.

Тезис доклада

О теоретико-автоматном подходе к эквивалентности ключей шифров.

В настоящее время теоретико-автоматный подход к анализу и синтезу шифров стал естественным и обычным направлением криптоанализа. Многие вопросы эквивалентности ключей шифров формулируются в форме неотличимости состояний выбранных автоматов. В докладе сообщается о полученной достижимой верхней оценки степени различимости связного перестановочного автомата с заданным диаметром.

Под словом автомат подразумевается конечный автомат $A=(X,S,Y,h,f)$, где:

X – конечное непустое множество, названное множеством входных символов (входной алфавит);

S – конечное непустое множество, названное множеством состояний (внутренний алфавит);

Y – конечное непустое множество, названное множеством выходных символов (выходной алфавит);

$h: S\times X\to S$ – функция переходов;

$f: S\times X\to Y$ – функция выхода;

$|X|, |S|, |Y|$ – мощности соответствующих алфавитов.

Если в момент времени $t\in\{1,2...\}$ автомат A находится в состоянии $s(t)\in S$, и на вход автомата поступил символ $x(t)\in X$, то в этот же момент времени на выходе автомата A образуется символ $f(s(t),x(t))$ и автомат A переходит в новое состояние $s(t+1)=h(s(t),x(t))$.

При условии, что $f(s,x)=\lambda(s)$ для любых $x\in X$, $s\in S$, где $\lambda: S\to Y$, автомат Мили A может рассматриваться как автомат Мура. Такой автомат будет обозначаться через $A=(X,S,Y,h,\lambda)$. Если множество X состоит из одного элемента $|X|=1$, то такой автомат называется автономным, и обозначается через $A=(S,Y,h,\lambda)$. Автомат часто задают его графом переходов: вершинами графа являются состояния автомата. Из каждого состояния s для каждого $x\in X$ проводится ориентированная дуга (стрелка $\to$) в состояние $s'=h(s,x)$. Она помечается двумя символами (x,y), где $y=f(s,x)$. Таким образом, из каждого состояния выходят $|X|$ дуг. Говорят, что состояние s' достижимо из s в автомате A, если в его графе переходов существует ориентированный путь из s в s'. Для таких пар состояний (s,s') вводят минимальное расстояние $m(s,s')$ от s до s', как минимальное число дуг, по которым можно перейти из s в s'.

Диаметром автомата A называют величину $\max\limits_{(s,s`)} m(s,s`)$, где максимум берется по всем парам состояний (s,s') таким, что существует расстояние $m(s,s')$. Граф переходов автомата (или просто, автомат) называют связным, если для любых его двух состояний s, s' в графе автомата существует неориентированный путь из состояния s в s'. Неориентированный путь это путь по состояниям графа переходов, использующий ориентированные дуги $\to$ и обратные к ним - $\leftarrow$. Если автомат не связный, то его граф переходов состоит из нескольких связных компонент – связных подавтоматов автомата. Автономный автомат $A=(S,Y,h,\lambda)$ называют полноцикловым, если его граф состоит из цикла, содержащего все его состояния. Граф переходов автомата (автомат) называют сильно связным, если для любой пары упорядоченных его состояний (s,s') существует ориентированный путь из s в s'. В любом связном автомате можно выделить сильно связный подавтомат автомата.

В дальнейшем предполагается, что рассматриваемый автомат A является связным с числом состояний $|S|\geq 2$. Кроме того, предполагается, что все его частичные функции переходов h_x осуществляют взаимнооднозначные преобразования множества S, то есть рассматриваемый автомат перестановочный (см [2]).

Формулировка основных результатов. Известна (см., например, [4, 1]) следующая достижимая оценка степени различимости R конечного автомата с числом состояний $|S|$

$$R\leq |S|-1.$$

Кроме того, в [3] было показано, что почти все автоматы имеют степень различимости равную $\log_{|X|} \cdot \log_{|Y|} |S|$.

Положим $N_0 = \{0,1,...\}$. В данной статье для произвольного связного перестановочного автомата с диаметром D доказана следующая оценка его степени различимости

$$R \le (l_0 + 1)(D+1) + \left[\frac{|S|}{2^{l_0+1}}\right] - 1,$$

где $[\nu]$ – целая часть числа ν, а l_0 – максимальное $l \in N_0$, если оно существует, при котором $\left[\frac{|S|}{2^l}\right] - \left[\frac{|S|}{2^{l+1}}\right] > D+1$, в противном случае $l_0 = -1$.

Данная оценка достижима для следующих параметров перестановочного связного автомата Мура:

1) $D = 1, \quad |S| = 3 \cdot 2^m, \ m \in N_0$;

2) $D = 1, \quad |S| = 5 \cdot 2^m, \ m \in N_0$;

3) $D = 2, \quad |S| = 5 \cdot 2^m, \ m \in N_0$.

Обозначим через $A(|S|, D)$ класс приведенных связных перестановочных автоматов Мура с числом состояний $|S|$, мощностью выходного алфавита $|Y| = 2$ и диаметром D. Доказаны следующие утверждения:

1) для любого автомата из класса $A(|S|, D)$, $|S| = 2(n+1)+1, \ n \in N_0$ тогда и только тогда $R < |S| - 1$, когда $D < n+1$;

2) для любого автомата из класса $A(|S|, D)$, $|S| = 4(n+1), \ n \in N_0$ тогда и только тогда $R < |S| - 1$, когда $D < 2(n+1)$;

3) Если для некоторого автомата из класса $A(|S|, D)$, $|S| = 4(n+1)+2, \ n \in N_0$

$$R = 4(n+1)+1,$$

то $D \ge 2(n+1)+2, \quad n \in N_0$.

Начальные результаты по данному направлению представлены в [5].

Литература

[1] Гилл А. Введение в теорию конечных автоматов // М.: Наука, 1966 — 272 с.

[2] Гинсбург С.В. О длине кратчайшего однородного эксперимента, устанавливающего конечные состояния машины // Кибернет. сб., №3. М., ИЛ, 1961. — С. 167 - 186.

[3] Коршунов А. Д. О степени различимости конечных автоматов // – Сб. тр. Дискретный анализ. Новосибирск: Наука, 1967, вып. 10. — С. 39 – 59.

[4] Мур Э. Ф. Умозрительные эксперименты с последовательными машинами// Сб. ст. Автоматы. М., ИЛ, 1956. — С. 179 -210.

[5] Бабаш А.В. Криптографические методы защиты информации// М.:РИОР ИНФРА-М, 2013.