«Инновационные технологии», Таиланд (Бангкок, Паттайа), 20-28 февраля 2013 г.

Технические науки

ВРЕМЕННЫЕ ДИСТРИБУТИВНЫЕ АСИНХРОННЫЕ АВТОМАТЫ

Кудряшова Е.С., Хусаинов А.А., Лошманов А.Ю.

ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет», Комсомольск-на-Амуре, e-mail: naj198282@mail.ru

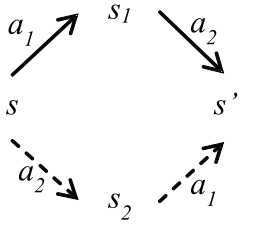
Дистрибутивным асинхронным автоматом называется пятерка (S, s_0, E, I, $Tran$), состоящая из множеств S и E, элемента $s_0 \in S$, отношения $Tran \subseteq S \times E \times S$ и семейства антирефлексивных симметричных отношений $I \subseteq (I_s)_{s \in S}$, $I_s \subseteq E \times E$. Должны быть выполнены следующие условия:

i Если $(s, a, s') \in Tran$ и $(s, a, s'') \in Tran$, то $s' = s''$

ii Для любых

$$s \in S, (a_1, a_2) \in I_s, (s, a_1, s_1) \in Tran,$$
$$(s_1, a_2, s') \in Tran,$$

существует такое $s_2 \in S$, что $(s, a_2, s_2) \in Tran$ и $(s_2, a_2, s') \in Tran$ (см. рисунок).



Аксиома (ii) для дистрибутивных асинхронных автоматов

Всякую асинхронную систему (S, s_0, E, I, $Tran$) можно рассматривать как дистрибутивный асинхронный автомат, полагая $I_s = I$ для всех $s \in S$.

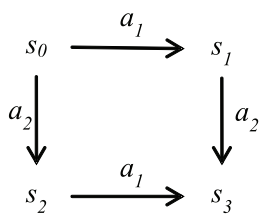
Определим сеть Петри как пятерку (P, T, pre, $post$, M_0), состоящую из конечных множеств P и T, функций $M_0: P \to \mathbf{N}$, $pre: T \to \mathbf{N}^P$, $post: T \to \mathbf{N}^P$. Здесь $\mathbf{N}^P$ обозначает множество всех функций $P \to \mathbf{N}$. Элементы $p \in P$ называются местами, $t \in T$ – переходами, $M \in \mathbf{N}^P$ – маркировками, а M_0 – начальной маркировкой. Определим отношение порядка на $\mathbf{N}^P$, полагая $M \le M'$, если для всех $p \in P$ верно $M(p) \le M'(p)$. Сумму и разность функций определим как $(M \pm M')(p) = M(p) \pm M'(p)$. Для $M, M' \in \mathbf{N}^P$ и $t \in T$ запись $M \xrightarrow{t} M'$ будет означать, что выполнены условия $M \ge pre(t)$ и $M' = M - pre(t) + post(t)$. В этом случае будем говорить, что маркировка M' получена из M с помощью срабатывания перехода t.

Пусть (P, T, pre, $post$, M_0) – сеть Петри. Обозначим $t = \{p \in P: pre(t)(p) \ne 0\}$. Сеть Петри ($P$, T, pre, $post$, M_0) определяет дистрибутивный асинхронный автомат (S, s_0, E, I, $Tran$), $S = \mathbf{N}^P$, $E = T$, $s_0 = M_0$, $Tran = \{(M, t, M') \in \mathbf{N}^P \times T \times \mathbf{N}^P$ существует $M \xrightarrow{t} M'\}$, для которого $I_m = \{(t_1, t_2) \in T \times T: M \ge pre(t_1)$ и $t_1 \cap t_2 = \varnothing\}$.

Временная сеть Петри это кортеж (N, eft, lft), где N – сеть Петри, eft: $T \to \mathbf{N}$, lft: $T \to \mathbf{N}$ – функции, описывающие соответственно раннее и позднее время доступности переходов, которые удовлетворяют ограничению $eft(t) \le lft(t)$ для каждого $t \in T$. Обобщим определение временной сети Петри. Обозначим через $\mathbf{R}_{\ge 0}$ множество всех неотрицательных вещественных чисел. Временным дистрибутивным асинхронным автоматом (A, eft, lft) называется дистрибутивный асинхронный автомат A = (S, s_0, E, I, $Tran$) вместе с парой функций eft: $E \to \mathrm{R}_{\ge 0}$, lft: $E \to R_{\ge 0} \cup \{\infty\}$, удовлетворяющих для всех $a \in E$ неравенству $eft(a) \le lft(a)$.

Введем временные состояния. Определим отображение $S \times E \to S \sqcup \{*\}$, полагая $s \cdot a = s'$, если $(s, a, s') \in Tran$. Если таких $s' \in S$ не существует, то положим $s \cdot a = *$. Временным состоянием временного дистрибутивного асинхронного автомата (A, eft, lft) называется пара (s, h) , состоящая из $s' \in$ мS и функции h: $E \to \mathbf{R}_{\ge 0} \cup \{\#\}$, таких что $s \cdot a \in S \Rightarrow h(a) \le lft(a)$ и $s \cdot a = * \Rightarrow h(a) = \#$. Каждое действие $a \in E$ имеет «часы». В начале работы временное состояние равно (s_0, h_0), где $h_0(a) = 0$, если существует $s' \in S$ и переход $s \xrightarrow{a} s'$.

Рассмотрим асинхронную систему, состоящую из двух независимых действий a_1 и a_2 и четырех состояний



для которых известные $ft(a_i)$ и $lft(a_i)$, $i \in \{1, 2\}$. Вычислим минимальное время выполнения операций, приводящих к состоянию s_3. Временные состояния (s, h) будем рассматривать как тройки (s_i, τ_1, τ_2). Пусть $eft(a_1) \le eft(a_2)$. Тогда возможен следующий путь выполнения:

$$(s_0, 0, 0) \xrightarrow{eft(a_1)} (s_0, eft(a_1), eft(a_1)) \xrightarrow{a_1} (s_1, \#, eft(a_1)) \xrightarrow{eft(a_2) - eft(a_1)} (s_1, \#, eft(a_2)) \xrightarrow{a_2} (s_3, \#, \#)$$

Легко видеть, что полученное время, равное сумме $eft(a_1) + eft(a_2) - eft(a_1)$ будет минимальным. Следовательно, в общем случае минимальное время будет равно max ($eft(a_1)$, $eft(a_2)$). Аналогично получим, что максимальное время выполнения действий будет равно max ($lft(a_1)$, $lft(a_2)$).

ПРИМЕНЕНИЕ ОЦЕНОК НА ОСНОВЕ ЭНТРОПИИ ДЛЯ СРАВНЕНИЯ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ

Сен Н.Д., Котляров В.П., Григорьев Я.Ю.

ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет», Комсомольск-на-Амуре, e-mail: naj198282@mail.ru

Объектом исследования являются методы криптографических преобразований данных. *Предмет исследования* – криптостойкость. Исходные данные представлены в виде цветного изображения в формате gif, 400×296 пикселей. Алгоритмы шифрования – гаммирование, DES, TripleDES, Rijndael; режимы шифрования – ECB, CBC, CFB. Поиск энтропии исходных и зашифрованных данных осуществляется по классической формуле Шеннона [2]. Выявлены два подхода к определению энтропии изображений (RGB):

– энтропия изображения находится как сумма энтропии каналов изображения;

– энтропия изображения вычисляется в зависимости от вхождений цветов в изображение.

В первом подходе [3] для расчета энтропии изображения H(X) необходимо определить энтропию каждого из каналов изображения. Пусть вектор C – канал изображения X, $C = \{R, G, B\}$. Тогда э*нтропия канала изображения* определяется по формуле Шеннона:

$$H(C) = \sum_{i=1}^{n} p_i \log_2 \left(\frac{1}{p_i} \right),$$

где C – канал изображения X; p_i – вероятность, определяемая как частное от деления количества появлений i-го байта ($i = 0...255$) в канале изображения C к числу байт канала C изображения X. Так как энтропия независимых источников равна сумме энтропии источников, то энтропия всего изображения $H(X)$ определяется как сумма энтропии каналов изображения:

$$H(X) = \sum H(C),$$

где C – канал изображения X, $C = \{R, G, B\}$.

В соответствии со вторым подходом энтропия изображения вычисляется по формуле Шеннона, однако вероятности определяются иным образом:

$$H(X) = \sum_{i=1}^{n} p_i \log_2 \left(\frac{1}{p_i} \right),$$

где X – изображение; p_i – вероятность, определяемая как частное от деления количества вхождений пикселя i-го цвета (RGB) к количеству пикселей изображения X.

Пусть $H_1(X)$ и $H_1(Y)$ – энтропии исходного и зашифрованного изображения, рассчитанные первым способом, а $H_2(X)$ и $H_2(Y)$ – вторым способом соответственно. Энтропия зашифрованного изображения, «зашумленного» ранее, рассчитанная первым и вторым способом – Hga1(Y) и Hga2(Y). Начальная энтропия $H_1(X) = 14{,}81$, $H_2(X) = 5{,}57$.

При использовании и первого, и второго способа расчета энтропии наблюдается схожая тенденция – шифрование в режиме ECB является наиболее «слабым», что подтверждается визуально. Наиболее «сильным» является шифрование DES, TripleDES, Rijndael в режиме CBC, при «зашумлении» исходных данных – Rijndael в режиме CBC. Энтропия Hga1(Y) и Hga2(Y) практически не меняется относительно $H_1(Y)$ и $H_2(Y)$, а в ряде случаев – значительно меньше. Таким образом, выполняемые преобразования над исходными данными существенно не добавляют вариации цвета изображения. Недостатком подхода является то, что энтропия не учитывает сложность формирования структуры данных и если изображение зашумлено, то оно всё равно формально обладает большим количеством информации [4]. Следовательно, оценивание на основе энтропии не является достаточным условием для принятия решений о стойкости криптопреобразований.

Список литературы

1. Вентцель Е.С. Теория вероятностей. – М., 2002.

2. Shannon, C. E A Mathematical Theory of Communication // Bell System Technical Journal, 1948.

3. Ковалев Д.С. Представление и сжатие данных // НГУ, спецкурс. – Режим доступа: http://nsu.videosoft.org/2010/tasks/task1/, свободный.

4. Бутенков С.А. энтропийный подход к оценке качества гранулирования многомерных данных // КИИ. – 2008.

О ПОРЯДКЕ, ПРАВИЛАХ И ОПЫТЕ СОСТАВЛЕНИЯ ТЕХНИЧЕСКИХ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ АУКЦИОНОВ В ЭЛЕКТРОННОЙ ФОРМЕ НА ОСНОВЕ ФЗ-94

Чудинов А.В., Трещёв И.А., Григорьева А.Л.

ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет», Комсомольск-на-Амуре, e-mail: naj198282@mail.ru

Люди не так ясно понимали механизмы контроля за процессом проведения аукционов. Но со временем, как и везде, в этой области многие придумали обходные пути, для того, чтобы закупать товары и услуги у предопределенного до аукциона поставщика. Придумывались хитрые технические задания, менялись цены в ходе вскрытия конвертов поставщиков, усложнялись условия осуществления конкурсов.