УДК 004.023

ИССЛЕДОВАНИЕ СТРУКТУРЫ ПРОСТРАНСТВА ОПИСАНИЯ ОБРАЗОВ ДЛЯ ФОРМИРОВАНИЯ СЕАНСОВЫХ КЛЮЧЕЙ

Галавинский В. А. Глущенко Ю. В. Глущенко В. Е.
Восточноукраинский Национальный Университет им. В. Даля г. Луганск
Кафедра компьютерные системы и сети
E-mail: kaf_kss@snu.edu.ua

Аннотация
Галавинский В.А., Глущенко В.Е., Глущенко Ю.В. Исследование структуры пространства описания образов для формирования сеансовых ключей*. В статье представлены результаты исследования структуры пространства линейных квазипорядков, необходимые для формирования сеансовых ключей.*

Общая постановка проблемы. В настоящее время одним из наиболее эффективных методов шифрования информации в процессе ее передачи является методы, основанные на концепции сеансовых ключей. Основное достоинство алгоритмов созданных при помощи данной методологии заключается в возможности использования различных ключей, для шифрования различных объемов данных в процессе их передачи.

В идеальном случае нужно, чтобы ключей было много, и они были бы достаточно разнообразны [1]. Поэтому проблема создания мощного математического аппарата, позволяющего формировать сеансовые ключи, а также обеспечивать базу для создания алгоритмов выборки этих ключей остается весьма актуальной.

Постановка задач исследования. Концепция формирования сеансовых ключей в структурированном пространстве была разработана на кафедре Компьютерных систем и сетей Восточноукраинского Национального Университета им. В. Даля и рассматривается в работе [1]. Реализация данной концепции обуславливает необходимость проведения исследования структуры пространства линейных квазипорядков, используемого для описания образов сеансовых ключей.

Решение задачи и результаты исследований. Для решения поставленной задачи был проведен анализ расположения точек смешанного потенциала на старших уровнях пространства линейных квазипорядков. Все основные понятия и определения, используемые далее, даны и описаны в работах [1,2].

Пусть точки смешанного потенциала образуют пространство QB. $QB \subset QL$. Множество HQB точек пространства QB определяется как:

$$HQB = \{R \mid R \in QL,\ \exists\ i,\ |R_i| > 1,\ |R_i + R_s| \geq 2\ \ i \neq s\}, \qquad (1)$$

где R_s - класс, определяющий потенциал ранжировки *R.*

Для исследования расположения точек смешанного потенциала в пространстве ранжировок введем следующие понятия.

Для описания структуры ранжировки, описывающей точку смешанного потенциала, будем пользоваться следующими условными обозначениями:

I_i^j - класс эквивалентности, мощность которого равна j, имеющий i-й порядковый номер в ранжировке;

R_i – одноэлементный класс, имеющий i–й номер в ранжировке.

Тогда ранжировка R=(a-b, c, d, e-f-g) , будет иметь следующий вид:

$$R = (I_1^2, P_2, P_3, I_4^3,).$$

Точки смешанного потенциала, отображающие разбиение множества A={a,b,…}, $|A|=N$, имеющие одинаковый потенциал равный U, образуют множество точек X_u.

$$X_u = \{R : \forall R \in HQB, Pot\ R = Pot\ U\}, \qquad (2)$$

где Pot U – значение потенциала гиперповерхности U, на которой расположены точки множества X_u.

Точки множества X_u с учетом структуры описываемых ранжировок, разбиваются на не пересекаемые подмножества, образующие уровни гиперповерхности.

Тогда

$$X_u = \prod_{i=1}^{R} Y_i, \quad Y_i \bigcap Y_j = O, \quad i \neq j.$$

При разбиении гиперповерхности на уровни используется информация о классе эквивалентности ранжировки, мощность которого без учета класса, определяющего потенциал точки, наибольшая.

Лемма 1. Для любой ранжировки $R = (k_1, k_2, ..., k_n)$, описывающей точку смешанного потенциала, на множестве A, существует класс

$$|k_u^R| \geq |k_i^R|, \quad i = 1,...,n, \quad i \neq u, \quad i \neq s,$$

где s – номер класса, определяющего потенциал ранжировки R.

Номер уровня, на котром располагается точка x, будем обозначать NuR.

Определение 1. Номер уровня, на котором располагается точка R, равен

$$NuR = |k_u| - 1.$$

Из определения 1 следует, что номер уровня, на котором располагается точка R, на единицу меньше мощности класса, определяющего номер уровня точки. Мощности классов, определяющие номер уровня двух точек одной гиперповерхности, расположенных на соседних уровнях, различаются на единицу. Мощность класса, определяющего номер уровня точек любого потенциала, расположенных на первом уровне, равна двум.

Так как наименьшее число классов, которое содержит ранжировка элементов множества A, описывающая точки смешанного потенциала, равно двум, то наибольшая мощность класса ранжировки, без учета класса, определяющего ее потенциал, при четном N равна N/2, при нечетном N равна (N+1)/2;

Следовательно, именно гиперповерхности этих потенциалов разбиваются на наибольшее число уровней.

Лемма 2. Максимальное число уровней, на которые разбиваются точки смешанного потенциала описываемые ранжировками элементов множества A мощностью $|A|=N$ равно, т.е.

$$\max 1N = \left[\frac{N}{2}\right] - 1. \qquad (3)$$

Очевидно, что количество гиперповерхностей точек смешанного потенциала, на которых расположены точки множества HQB при четном N будет нечетно. Потенциал гиперповерхности, множество точек которой разбивается на наибольшее количество уровней равно N/2. Точки этой гиперповерхности, расположенные на max lN уровне, описываются дихотомическими разбиениями, включающиеми класс RS, определяющий потенциал точки и класс Ru, определящий номер уровня, мощности которых равны:

$$|R_s| = |R_u| = \frac{N}{2}.$$

При убывании значения потенциала у гиперповерхностей, потенциалы которых находятся в пределах от N-2 до N/2, на единицу, число уровней, на которые разбиваются точки данной гиперповерхности, увеличивается на единицу. Это обуславливается тем, что уменьшение на единицу мощности класса, определяемого потенциалом точки, позволяет увеличить мощность класса, определяющего номер уровня, также на единицу. Такое уменьшение мощности класса, определяемое потенциалом точки, и увеличение мощности класса, определяющего номер уровня точки, проводиться до тех пор, пока их мощности не станут равными.

При изменении на единицу значения потенциала у гиперповерхности, потенциал которой находится в пределах от N/2 до 2, на единицу, число уровней, на которые разбивается множество точек данной гиперповерхности, уменьшается на единицу. Это обуславливается условием леммы 1, согласно которого, мощность класса, определяющего потенциал точки, не меньше мощности любого класса разбиения. Следовательно, уменьшение мощности класса, определяющего потенциал, на единицу повлечет за собой уменьшение на единицу мощности класса, определяющего номер уровня.

Из вышесказанного вытекает справедливость следующего утверждения.

Утверждение 1. Число уровней, на которые разбивается гиперповерхность точки смешанного потенциала U при четном N, $N = |A|$, равно:

$$e'_N = \begin{cases} N - PotU - 1, \text{ если } PotU \geq \dfrac{U}{2} \\ PotU - 1, \text{ если } PotU < \dfrac{U}{2} \end{cases}$$

При нечетном N, $N = |A|$, количество гиперповерхностей, т.е. потенциалов четно. Потенциалы гиперповерхностей, множество точек которых разбиваются согласно (2.1.3) на max lN уровней, равны:

$$\frac{N-1}{2} \text{ и } \frac{N+1}{2};$$

Тогда на гиперповерхности U_1, Pot $U_1 = (N+1)/2$, точки уровня имеющего номер max lN, описываются дихотомическими разбиениями для которых справедливо:

$$|R_s| - |R_u| = 1.$$

Точки гиперповерхности U_2 , Pot $U_2=(N-1)/2$, расположенные на уровне номера max lN, описываются ранжированием включающими три класса. Двумя из этих классов являются классы Rs и Ru , для которых $|Rs| = |Ru|$, и один одноэлементный класс.

Тогда, при убывании значения потенциала на единицу у гиперповерхности, потенциал которых находится в пределах от N-2 до (N-1)/2, число уровней на которые разбиваются точки данной гиперповерхности, увеличивается на единицу. Это обуславливается тем, что уменьшение на единицу мощности класса, определяющего потенциал точки, позволяет увеличить на единицу мощность класса, определяющий номер уровня точки. Такое уменьшение мощности класса, определяющей номер точки, и увеличение мощности класса, определяющего номер уровня, может быть проводиться до тех пор, пока не станет справедливой разность.

$$|R_s| - |R_u| = 1$$

При изменении на единицу значений потенциала у гиперповерхностей, потенциалы которых находятся в интервале от (N-1)/2 до 2,

Из вышеизложенного вытекает справедливость следующих утверждений.

Утверждение 2. Число уровней, на которое разбивается гиперповерхность точек смешанного потенциала U при нечетном N, $|A|=N$, равно

$$e_N^H = \begin{cases} U - PotU - 1, & \text{если } PotU \geq \dfrac{N+1}{2} \\ PotU - 1, & \text{если } PotU < \dfrac{N-1}{2} \end{cases} \qquad (4)$$

Упростим выражения (3) и (4) для нахождения числа уровней, на которые разбивается гиперповерхность любого потенциала.

Лемма 3. Число уровней, на которые разбивается гиперповерхность U точек смешанного потенциала при четном N равно.

$$l_N = \left[\frac{N}{2}\right] - 1 - \left(\left|\left[\frac{N}{2}\right] - PotU\right|\right). \qquad (5)$$

Лемма 4. Число уровней, на которое разбивается гиперповерхность U,

$$Pot\ U \neq \frac{N-1}{2},$$

точек смешанного потенциала при нечетном N равно:

$$l_N = \left[\frac{N}{2}\right] - 1\left(\left|\left[\frac{N}{2}\right] - PotU\right|\right). \qquad (6)$$

Теорема. Число уровней, на которые разбивается гиперповерхность U, точек смешанного потенциала равна:

$$l_n = \begin{cases} \left[\dfrac{N}{2}\right] - 1 - \left(\left|\left[\dfrac{N}{2}\right] - PotU\right|\right), & \text{если } PotU \neq \dfrac{N+1}{2} \text{ при нечетном } N \\ \dfrac{N}{2} - 1, & \text{если } PotU \neq \dfrac{N+1}{2} \text{ при четном } N \end{cases}$$

Все точки гиперповерхности заданного потенциала одного уровня разбиваются на соответствующие подмножества, образующие орбиты данного уровня. Разбиение (уровня) точек на орбиты производится с учетом количества двухэлементных классов, входящих в ранжировки, описывающие рассматриваемые точки. При этом классы, определяющие потенциал точек и номер их уровня, не влияют на номер орбиты.

Номер орбиты, на которой располагается точка R, будем обозначать NoR.

Определение 3. Номер орбиты, на которой располагается точка смешанного потенциала $R=(R_1,\ldots,R_m)$ равен

$$NoR = \sum_{i \in Q} \frac{|R_i|}{2} + 1;\ Q = \{i \mid |R_i| = 2,\ i = 1,\ \ldots,\ m,\ i \neq s,\ i \neq u\} \qquad (7)$$

где R_s- класс, определяющий потенциал точки R, R_u – класс, определяющий номер уровня, на котором расположена точка R.

Из определения 2, 3 следует, что на первом уровне первой орбиты гиперповерхности любого потенциала, располагаются точки смешанного потенциала, описываемые ранжировками не содержащими ни одного класса мощностью, равной двум, не считая классов, определяющих потенциал точки и номер уровня, на котором они расположены.

Количество двухэлементных классов в ранжировках, описывающих пару точек равного потенциала и уровня, расположенных на соседних орбитах, различаются на единицу.

Выведем выражения, позволяющие определять максимальное число орбит, на которые разбиваются точки заданного уровня определенной гиперповерхности.

Пусть ранжируются объекты множества A=(a,b,c…), мощность которого равна N. Количество элементов, из которых будут формироваться двухэлементные классы при переходе от одной орбиты на другую на гиперпоперхности U, i-го уровня, равно N - PotU-(i+1). Так как точки первой орбиты описываются ранжировками, которые содержат не считая класс, определяющий потенциал ранжировки, и класс, определяющий номер уровня, лишь одноэлементные классы, то, следовательно, справедлива следующая лемма.

Лемма 5. Число орбит, на которые разбиваются i-й уровень гиперповерхности U, равно

$$r^i = \left[\frac{N - PotU - (i+1)}{2} \right] + 1. \qquad (8)$$

Здесь квадратные скобки обозначают целую часть от числа.

Из определения 3 следует, что на первом уровне первой орбиты гиперповерхности любого потенциала, располагаются точки смешанного потенциала, описываемые ранжировками не содержащими ни одного класса

Выводы.

Результаты исследования структуры гиперпростпанства, выбираемого в качестве пространства описаний сеансовых ключей, образуют поле знаний для реализации аппарата распознавания, основанного на использовании геометрического подхода к нахождению групповых решений.

Список литературы

1. Глущенко В.Е. Глущенко Ю.В Методика формування сеансових ключів //. Вісн. Східноукр. нац. ун-т. ним В. Даля - Луганськ. - 2009. - № 6. - с.23-28

2. Глущенко В.Е., Глущенко Ю.В. Концептуальные вопросы построения интеллектуальных систем защиты от несанкционированного доступа. // Вістник Східноукраїнського національного університету ім. Володимира Даля. - 2006. - № 5 [111] - с.48-53.