Дослідження структури простору опису образів сеансових ключів

В.Є. Глущенко
кафедра кібернетики та комп'ютерних систем
Східноукраїнський національний університет
імені В.Даля
Сєвєродонецьк, Україна
2847@i.ua

М.Л. Петришин
кафедра інформатики
Прикарпатський національний університет
імені Василя Стефаника
Івано-Франківськ, Україна
M.L.Petryshyn@gmail.com

Investigation of the space structure of session keys patterns description

V. Glushchenko
Department of Cybernetics and Computer Systems
Volodymyr Dahl East Ukrainian National University
Severodonetsk, Ukraine
2847@i.ua

M. Petryshyn
Department of Computer Science
Vasyl Stefanyk Precarpathian National University
Ivano-Frankivsk, Ukraine
m.l.petryshyn@gmail.com

***Анотація*—В статті представлено результати дослідження структури простору лінійних квазіпорядків, необхідних для формування сеансових ключів**

***Abstract*—The article presents the research results on the structure of the linear space quasiparallel necessary for creating session keys**

***Ключові слова*—інформаційна безпека, сеансові ключі, завадостійкість, кодування, інформація**

***Keywords*—information security, the session key, noise resistance, encoding information**

I. INTRODUCTION

As the latest research of domestic and foreign authors, one of the most effective methods of encrypting data during its transmission is a method based on the concept of session keys. Therefore, the problem of creating a powerful mathematical apparatus allows you to create a variety of session keys and provides the basis for the creation of effective algorithms working with these keys remains highly relevant.

II. FORMULATION OF RESEARCH PROBLEMS

The formation concept of session keys in a structured space is considered in [1, 2]. Implementation of this concept makes it necessary to study the structure of linear space quasi orders used to describe the images of session keys.

III. THE RESEARCH RESULTS

To solve this problem the location points of the mixed potential at the senior levels of the space of linear quasi-orders were analyzed. All the basic concepts and definitions used below, and are described in following work [1].

Let the points form a mixed potential space QB, $QB \subset QL$. Multiple HQB points of QB points is define as:

$$HQB=\{R|\ R\in QL,\ \exists i,\ |Ri|>1,\ |Ri+Rs|\geq 2\ i\neq s\}, \quad (1)$$

where R_s - class that defines the potential rankings R.

To investigate the combined potential points location in ranking space are introduced the next concepts.

To describe the ranking structure, that describes mixed-point potential, we use the following reference designation: I_i^j - equivalence class, whose power is equal to j, having the i-th serial number in the ranking; P_i - single element class that has the i-th number in the ranking.

Then the ranking of $R=(a\text{-}b,c,d\text{-}e\text{-}f,g)$ will have the following form: $R=(I_1^2P_2I_3^3P_4)$.

Points of mixed potential, showing a partition of set $A=\{a,b,\ldots\}$, $|A|=N$, having the same potential equal to U, form a set of points X_u.

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

where *Pot U* – the value of the potential hypersurface *U*, where located points of set X_u.

The point of X_u set with considering structure of described rankings are divided into disjoint subsets forming a level surface. Than $X_u=\prod_{i=1}^{R} Y_i$, $Y_i \cap Y_j=\varnothing$, $i\neq j$.

When splitting the hypersurface at the levels is used the information about class rankings equivalence which capacity without taking into account the class, which determines the potential of the point, the greatest.

Lemma 1. For any ranking $R=(k_1, k_2, ..., k_n)$, which describes the point of the mixed potential on *A*, there is a class $|k_u^R| \geq |k_i^R|$, $i=1, ..., n$, $i\neq u$, $i\neq s$, $u\neq s$, where *s*-class number, which determines the potential of the rankings *R*. The level number, where located the point *x* will be denoted by *NuR*.

Definition 1. The level number, where the *R* point is located, is equal $NuR=|k_u|-1$.

From Definition 1 follows that the number of levels on which the point of the *R*, one less than the capacity of the class that defines the level of the point number. Power classes, defining the number of levels of two points of one hypersurface located on adjacent levels differ by one. Power class defines the number of points the level of any building, located on the ground level, is equal to two.

As the smallest number of classes, which contains the ranking of elements of *A*, which describes the point of the mixed potential, is equal to two, the greatest power of class rankings, excluding the class that defines its potential for even *N* is equal to *N/2* when *N* is odd is equal to *(N+1)/2*.

Therefore, it is a hypersurface of the potential split in the largest number of levels.

Lemma 2. The maximum number of levels, which are divided points of mixed potential elements described rankings of *A* power $|A|=N$ is equal, i.e.

$$\mu\alpha\xi\, \lambda_N=\left[\frac{N}{2}\right]-1 \qquad (3)$$

It is obvious that the number of hypersurfaces points of mixed potential, on which there are points of *HQB* for even *N* is odd. The potential hypersurface whose set of points is divided into the greatest number of levels equal to *N/2*. The points of this hypersurface located on max l_N level described dichotomous partitions, that include the class of the R_S, which determines potential of the point and the class of R_u, determined by the level number, the power of which are:

$$|R_S| = |R_u| = N/2.$$

With decreasing values of the potential at the hypersurface whose potentials are in the range from *N–2* to *N/2* unit, the number of levels into which hypersurface this point is incremented. This is due to the fact that the decrease in unit performance class determined the potential points can increase the capacity of the class, which determines the level number, and per unit.

When changing value per unit potential of the hypersurface whose potential is in the range of *N/2* to *2* per unit, the number of levels into which the set points of the hypersurface is decremented. This is due to the condition of Lemma 1, according to which class power determines the potential of points, is not less than the power of any class of the partition.

From the foregoing, it follows the following assertion.

Assertion 1. The number of levels into which a hypersurface points of the mixed potential *U* for even *N*, $N=|A|$, equal to:

$$e_N^r = \begin{cases} N - PotU - 1, & if \quad PotU \geq \dfrac{U}{2} \\ PotU - 1, & if \quad PotU < \dfrac{U}{2} \end{cases}.$$

For odd *N*, $N=|A|$, the number of hypersurfaces, i.e., even potential. Potentials hypersurfaces, the set of points that are divided by (3) at *max* l_N levels, and are equal to (*N*–1)/2 and (*N*+1)/2;

Then on the hypersurface U_1, *Pot* $U_2=(N–1)/2$, the level of points having a number of *max* l_N, described dichotomous partitions for which holds: $|Rs|-|R_u|=1$.

U_2 hypersurface point, *Pot* $U_2=(N–1)/2$, located at the level of numbers *max* l_N, describes three classes comprising ranking. Two of these classes are classes R_s and R_u, which $|R_s|=|R_u|$, and one singleton class.

With the decrease of potential values per unit of the hypersurface whose potential is in the range of *N–2* to the number of levels into which the points of this hypersurface is incremented. This is due to the fact that the decrease per unit of class power determines the potential of points, can increase the power per unit class, which determines the level of the point number.

From the foregoing it follows that the following claims.

Assertion 2. The number of levels into which divided the hypersurface mixed potential points *U* for odd *N*, $|A|=N$, is equal to

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

Simplifying the expression (3 and 4) to find the number of levels into which divided any potential hypersurface.

Lemma 3. The number of levels into which divided the hypersurface *U* mixed potential outlets for even *N* is

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

Lemma 4. The number of levels into which divided the hypersurface *U*, *Pot U*, mixed potential points when *N* is odd

$$l_{N=}\begin{cases}\left[\frac{N}{2}\right]-1-\left(\left[\frac{N}{2}\right]-PotU\right) & if\ PotU \neq \frac{N+1}{2} \quad when\ N\ is\ even \\ \frac{N}{2}-1 & if\ PotU \neq \frac{N+1}{2} \quad when\ N\ is\ odd\end{cases}$$

All points given potential hypersurface one level are divided into subsets corresponding to that form of the orbit of this level. Partitioning (level) of points on the orbit is made with regard to the number of two-element classes included in the ranking, describing the points under consideration. At the same classes that define the potential points and their level number, do not affect the orbit number.

The orbit number, on which the point *R* will be denoted *NoR*.

Definition 3. The orbit number, on which is the point of the mixed potential $R=(R_1,...,R_m)$ is equal to:

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

where R_S-class that defines the potential of points *R*, R_U- class, which determines the number of levels on which the point *R*.

From the definition 3 follows that the first level of the first hypersurface orbit of any potential, located points of the mixed potential, described rankings do not contain any class of power, equal to two, not including classes, defining the points and the potential number of levels on which they are located.

The number of two-element classes in the rankings, describing a couple of points of equal potential and level, located on adjacent orbits differ by one.

Let derive expressions for defining the maximum number of orbit into which divide a certain level of points given hypersurface.

Let ranked objects sets *A=(a,b,c ...)*, whose power is equal to *N*. The number of elements of which will be formed

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

Theorem. The number of levels into which divided the hypersurface of the *U*, a mixed potential points is equal to:

two-element classes during the transition from one orbit to another on hypersurface *U*, *i*-level, equal to *N–PotU–(i+1)*. As the first point of the orbit described by the rankings, which contain apart from the class, which determines the potential of the rankings, and the class that defines the level number, a single-element classes, it follows that the following lemma holds.

Lemma 5. The number of orbits into which the *i*-th level of the *U* hypersurface, is equal to

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

Here the square brackets denote the integer part of the number.

The definition 3 it follows that on the first level of the first hypersurface orbit of any potential, located in terms of the mixed potential, described rankings do not contain any class.

CONCLUSION

Results of the study hypersurface structure selected as a space descriptions session key images form a field of knowledge, to recognize the device, based on the use of the geometric approach to finding solutions group.

REFERENCES

[1] В.Е. Глущенко, Ю.В. Глущенко Методика формування сеансових ключів. Вісн. Східноукр. нац. ун-т. В.Даля, -Луганськ. - 2009. -№6, Ч.1. –С. 189-193.

[2] В.Є. Глущенко, М.Л. Петришин Формування завадостійкого коду сеансових ключів. Матеріали статей п'ятої Міжнародної науково-практичної конференції "Інформаційні технології та комп'ютерна інженерія", - Івано-Франківськ. 2015. – с.171–174.