Дослідження Розташування Образів Сеансових Ключів на Старших Рівнях Гіперпростору Описів

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

Михайло Петришин
кафедра інформатики
Прикарпатський національний університет
Івано-Франківськ, Україна
m.l.petryshyn@gmail.com

Investigation of the Images Session Keys Location at the Higher Levels of Hyper-Space Descriptions

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

Mykhailo Petryshyn
dept. of Computer Science
Precarpathian National University
Ivano-Frankovsk, Ukraine
m.l.petryshyn@gmail.com

***Анотація*—
Устаттіпредставленірезультатидослідженняструктурипростолінійнихквазіпорядків, необхіднідляформуваннясеансовихключів, що є одним з найбільш ефективних методів шифрування інформації в процесі її передачі**

***Abstract*—The article presents the results of the study of the structure of the space of linear quasiorders, which are necessary for the formation of session keys, which is one of the most effective methods of encryption of information in the process of its transmission**

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

Keywords—information security, session keys, noise immunity, encoding, information.

I. Вступ

Дослідження вітчизняних і зарубіжних авторів показують, що найбільш ефективних методів шифрування інформації в процесі її передачі є методи, засновані на концепції сеансових ключів. Тому проблема створення потужного математичного апарату, що дозволяє формувати різноманітні сеансові ключі і забезпечує базу для створення ефективних алгоритмів роботи з цими ключами, залишається досить актуальною.***Постановка задач дослідження.*** Концепція формування сеансових ключів в структурованому просторі розглядається в роботах [1,2]. Реалізація даної концепції виникає нагальна потреба дослідження розташування образів сеансових ключів на старших рівнях гіперпростору їх опису.

II. Результати дослідження

У даній роботі представлені результати досліджень розташування точок змішаного потенціалу на старших рівнях гіперповерхні. Всі основні поняття і визначення, що використовуються далі, наведені та описані в роботах [1,2].

Нехай точки простору *QB* відображають впорядкованумножину $A = \{a, b, ...\}$, $|A| = N$, $N > 4$.Вони описуються ранжуванням змішаного потенціалу і утворюють множину*HQB*. Позначаємо через *HC*множину всіх точок, розташованих на старших рівнях гіперповерхні, потенціали яких змінюються від *2* до $N - 2$,$HC \subset HQB$.

Точки, що входять в множину*HC*, описуються дихотомічними розбиваннями. Нехай точки старшого рівня гіперповерхні U утворюють множину $HB_u \subset HC$. Тоді потужність множини *HB* дорівнює

$$\left|HB_u\right| = 2\frac{M!}{Pot\ U!\left(N - Pot\ U\right)!} \qquad (1)$$

Будемо позначати через δ потужність класу, що визначається номера рівня, на якому, розташовуються аналізовані точки. Значення δ для гіперповерхні *U*рівнеl_{N+1}, де l_N визначається з виразу 2.

$$l_N = \begin{cases} \left[\frac{N}{2}\right] - 1 - \left(\left[\frac{N}{2}\right] - PotU\right) \\ \frac{N}{2} - 1 \end{cases} \quad (2)$$

Так як $\forall R \in HBu$описуються дихотомічними розбивками, то потужність класу, що визначає потенціал $R \in HBu$, буде дорівнює $N - \delta$.Тоді вираз (1) може бути записано у вигляді:

$$|HBu| = 2\frac{M!}{(N-\delta)!\delta!} \quad (3)$$

Розіб'ємо множину*HC* на дві підмножини так, що

$$HA = \{R : R \in HC;\ PotP = N/2\},\ HB = HC / HA.$$

Тоді в підмножині*HA* увійдуть ті ж точки, які описуються розбивками, у яких потужність класів, що визначає потенціал і визначає номер рівня, рівні. У підмножину*HB* - точки, у яких потужності цих класів не рівні.

Розглянемо точки множини*HB*. Точки цієї множини описуються дихотомічними розбивками, в яких потужність класу, що визначає потенціал цих точок, завжди більше потужності класу, що визначає номер рівня на якому розміщуються ці точки.

Нехай *HBu* утворюють точки гіперповерхні *U, Pot U = N* - δ рівня, з номером l_N,, де l_N визначається з виразу (2).

Розіб'ємо *HBu* на підмножини однотипних точок

$$NB_U^1 \subset HB_U,\ NB_U^2 \subset HB_U : NB_U^1 \cap NB_U^2 = 0,\ NB_U^1 \cup NB_U^2 = HB.$$

Виведемо вираз для знаходження відстаней між сусідніми і взаємно протилежними точками множини*HBu*.

Нехай точка $R \in HB$, описується дихотомічною розбивкою$R = (I^{N-\delta} I^{\delta})$і розташовуються на гіперповерхні *U, Pot U = N* - δ.тоді $|K_S^R| = N - \delta$, $|K_U^R| = \delta$.

Розглянемо вирази, що визначають абсолютні відстані для сусідніх точок *R* і *P*, з урахуванням потужності класів K_S^R та K_U^R

Нехай для точки R справедливо $|K_S^R| - |K_U^R| = 1$. Виведемо з K_S^Rелемент *x* і введемо його в клас K_U^R. Тоді

$$D = K_S^R / x,\ |D| = \delta,\ C = K_U^R \cup x,\ |c| = N - \delta.$$

Отримана при цьому точка *P* описується ранжуванням виду

$P = (I^{\delta} I^{N-\delta})$. Точка $P \in HB,\ Pot\ P = N - \delta$,

отже вона лежить на тій же гіперповерхні, що і точка *R* і є сусідньою з нею.

Абсолютна відстань між *R* і *P*рівна:

$$d(R, P) = (N - \delta - 1) + \delta = N - 1 \quad (4)$$

Точки *R* і *P* описуються однотипними дихотомічними розбивками, для яких справедливо:

$$K_S^R \cap K_S^P \neq 0,\ |K_S^R \cap K_S^P| = 1, K_S^P \subset K_S^R : K_S^R \subset K_S^P$$

Лемма 1. Відстань між сусідніми точками *R* і *P* $|K_S^R \cap K_S^P| = 1,\ |K_S^R| - |K_u^R| = 1$ рівно *d(R, P) = N* – 1.

Нехай для точки *R* справедливо $|K_S^R| - |K_u^R| = 2$ Тоді отримання з *R* інших точок, розташованих на тій же гіперповерхні, що і точка *R* можливо двома способами. розглянемо кожен з них окремо.

1. Так як $|K_S^R| - |K_u^R| = 2$, то для отримання точки P_i, $P_i \in HB$, $Pot\ P_i = Pot\ R$, описуваної однотипним з R дихотомічним розбиттям, виведемо з K_S^R елемент *x*, $D = K_S^R / x$. Із K_U^R виведемо елемент у C= K_U^R / y, $D = K_S^R / c$, |*D*| = 2. Поміняємо елементи *x* і *y* місцями. отримуємо

$$K_S^{Pi} = D \cup y, K_U^{Pi} = D \cup x.$$

При виконанні цієї процедури *N-δ-1+δ-1* відносин еквівалентності було замінено на відносини строгого порядку, δ - 1 + *N* - δ - 1 проте відношення строгого порядку - на відношення еквівалентності, і відношення строгого порядку між елементами *x* і *y* зміні на протилежне. Отже, абсолютна відстань між точками *R* і P_iрівна

$$d(R, P) = 2(N - \delta - 1 + \delta - 1) + 2 = 2N - 2 = 2(N - 1) \quad (5)$$

2. Розглянемо другий спосіб отримання точки *P*, що лежить на тій же гіперповерхні, що і точка *R*. Виведемо з K_S^R двох елементний клас еквівалентності *C*, $D = K_S^R / c$, $|D| = 2$. Об'єднаємо класи $K_S^R \cup C$, $|K_S^R \cup C| = N - \delta$. Отримана точка *P*, описується ранжуванням $P = (I^{\delta} I^{N-\delta})$.Вона лежить на тій же гіперповерхні, що і точка *R*. Абсолютна відстань між точками *R* і *P*рівна

$$d(R, P) = 2(N - \delta - 2) + 2\delta = 2(N - 2) \quad (6)$$

Порівнюючи відстані між точками *R*, P_iта *R*, *P*отримуємо $d(R, P) > d(R, P_i)$,отже точка P_i не є сусідньою точці *R*, а точка *P* сусідня точці *R*.

Сусідні точки *R* і *P* описуються однотипними дихотомічним розбиванням, для яких справедливі відношення:

$$K_S^R \cap K_S^P \neq 0,\ |K_S^R \cap K_S^P| = 1, K_S^P \subset K_S^R : K_S^R \subset K_S^P$$

Лемма 2. Відстань між сусідніми точками *R* і *P* $|K_S^R \cap K_S^P| = 2,\ |K_S^R| - |K_u^R| = 2$ рівна*d (R, P) = 2 (N - 2).*

Нехай для *R* справедливо $|K_S^R| - |K_u^R| > 2$. Тоді для отримання з *R* інших точок, розташованих на тій же гіперповерхні, що і точка *R*, розглянуті вже використовувані способи.

1. Так як, $\left|K_S^R\right| - \left|K_u^R\right| = n$, $n > 2$, то для отримання точки $P \in HB$, $Pot\ R = Pot P$описуваної однотипним дихотомічним розбиттям з R виведемо з K_S^R елемента x, а з K_U^R - елемент y іx поміняємо їх місцями. Тоді абсолютна відстань між R і Pрівна:

$$d(R, P) = 2(N - 1)$$

2. Для отримання точки P_i, що описується не однотипним дихотомічним розбиттям з R з K_S^R виводимо клас K_1, $|\ K_1\ | = \delta$, $C = K_S^R / K_1$.. Об'єднаймо $K_U^R \cap C = K_S^P$. При цьому відношенням еквівалентності у $(N - \delta - \delta)\delta$ пар елементів зміняться на відношення строгого порядку. Відношення строгого порядку у у $(N - \delta - \delta)\delta$ пар елементів зміняться на відношення еквівалентності. Таким чином, загальне число пар елементів, у яких змінилися відношення, так само $2\delta(N - 2\delta)$, отже, абсолютна відстань між R і P_i рівно

$$d(R, P_i) = 2\delta(N - 2\delta) \qquad (7)$$

Порівнюючи відстань між R, P і R і P_i отримуємо, що $d(R, Pi) > d(R, P)$ отже, точка P_i не є сусідньою точці R, точка P - сусідня точці R.

Отримуємо точки R і P однотипними дихотомічними розбиттями, для яких справедливо:

$$K_S^R \cap K_S^P \neq 0,\ K_U^R \cap K_U^P \neq 0,\ \left|K_S^R \cap K_S^P\right| = 1.$$

Лема 3. Відстані між сусідніми точками R і P $\left|K_S^R\right| - \left|K_S^P\right| > 2$, $\left|K_S^R \cap K_S^P\right| = 1$ рівна$d(R, P) = 2(N - 1)$.

Теорема 1. Відстань між сусідніми точками змішаного потенціалу Rи P, R, $P \in HB$, старшого рівня гіперповерхні U, $Pot\ U = N - \delta$ рівна:

$$d(R, P) = \begin{cases} N - 1, & \text{якщ} \left|K_S^R\right| - \left|K_S^P\right| = 1 \\ 2(N - 2), & \text{якщо} \left|K_S^R\right| - \left|K_S^P\right| = 2 \\ 2(N - 1), & \text{якщо} \left|K_S^R\right| - \left|K_S^P\right| > 2 \end{cases} \qquad (8)$$

Справедливість теорема випливає з умови лем 1, 2, 3.

Теорема 2. Відстані між взаємно зворотними точками старшого рівня гіперповерхні $N - \delta$ при $N > 4$ рівна $2\delta(N - \delta)$.

Доведення. Нехай R і P два дихотомічні ранжирування елементів множини A, $N = |\ A\ |$, $N > 4$, Nнепарне, описує взаємно зворотні точки змішаного потенціалу $N - \delta$. Класи, що визначають потенціал даних ранжування, рівні і мають різні номери. Для отримання ранжування P з ранжуваннямR, необхідно поміняти сетами класи ранжування R. При цьому відношення старого порядку у $(N - \delta)\ \delta$ пар елементів замінюється на протилежне відношення. Отже, число незбіжних елементів у відповідних матрицях парних порівнянь дорівнює $2(N - \delta)\ \delta$,, тобто відстань між R і Pрівна$d(R, P) = 2\delta$ $(N - \delta - 1)$, що й треба було довести.

Розглянемо точки множиниHA. Точки даної множини описуються ранжуванням, у яких потужність класу, що визначає потенціал ранжування, дорівнює потужності класу, що визначає номер рівня, на якому розташована точка, описувана цим ранжуванням. Нехай $N = |\ A\ |$ - парне. Тоді точки множиниHA описуються дихотомічними ранжуваннями. МножинуHA розіб'ємо на підмножини однотипних точок

$$HA^1 \subset HA,\ HA^2 \subset HA : HA^1 \bigcap HA^2 = 0;\ HA^1 \bigcup HA^2 = HA.$$

Номер рівня, на якому розташовані точки множини HA дорівнює$l_N = \left[\frac{H}{2}\right] - 1$.

Лемма 4. Відстань між сусідніми точками старшого рівня гіперповерхні потенціалу $N / 2$ при парномуN, $N > 4$ дорівнює $2(N - 1)$.

Доведення. Нехай Rи P, $R \in HA^1$, $D \in HA^2$, сусідні точки, $Pot\ R = Pot\ P = N/2$. Так як, точки R і P описуються дихотомічними розбиваннями, то потужність класу R_1, що визначає номер рівня точки P, дорівнює потужності класу P_U, що визначає номер рівня точки P, при чому $|\ R_U\ | = |\ P_U\ | = N/2$.

Нехай $R_S \bigcap P_U = Q;\ R_U \bigcap P_S = b.$ Тоді для отримання відношенняD з R виведемо елемент а R_Sотримуємо сегмент $C^1 = R_S / a$. При цьому відношення еквівалентності у $(N / 2 - 1)$ пар елементів зміниться на відношення строгого порядку. З класу R_U виведемо елемент b, отримуємо сегмент $C^2 = R_U / b$.. При цьому відношення еквівалентності у $(N / 2 - 1)$ пар елементів зміниться на відношення строгого порядку.

Введемо елемент a в сегмент C^2. При цьому відношення строгого порядку у $(N / 2 - 1)$ пар елементів зміниться на відношення еквівалентності. Аналогічне відбувається при введенні елемента b в сегмент C^1. Ставлення строгого порядку між елементами a і b зміниться на протилежне. Отже, загальна кількість пар, у яких змінилися відношення дорівнює $4(N / 2 - 1) + 2 = 2(N - 1)$ що й треба було довести.

Лемма 5. Відстань між сусідніми точками $\left(\frac{N-1}{2} - 1\right)$ рівня гіперповерхні потенціал $\frac{N-1}{2}$ при потужності N, $N > 4$, рівно $2\left(2\left[\frac{N}{2}\right] - 1\right)$

Доведення. Нехай ранжуваннямR і P описуються точки, $Pot\ R = Pot\ P = \frac{N-1}{2}$: Вони містять три класи, якими є: клас, який визначає потенціал; клас, який визначає номер рівня; одноелементний клас. При цьому $\left|R_3\right| = \left|R_U\right| = \left|R_3\right| = \frac{N-1}{2}$; Так як точки R і P сусідні, то класи R_bи R_U и классиP_bи P_U, знаходяться в ранжуванні по сусідству. При цьому елементи, що містяться в одноелементних класах ранжування R і P, збігаються, а самі класи мають один і той же номер в цих ранжуваннях. Так як відстань між точками не залежить від співпадаючих частин ранжування, що описують ці точки, то отже R і P

відрізняються лише на сегментах $C_1 = (R_S, P_U)$, $C_2 = (P_U, P_S)$. Так як ці сегменти описуються дихотомічними розбивками, а кількість вхідних в них елементів парне, то з леми 2.6. отримуємо, що $d(R,P) = 2\left(2\left[\frac{N}{2}\right]-1\right)$, що й треба було довести.

Узагальнюючи леми 4. і 5. отримуємо $2(N-1) = 2\left(2\left[\frac{N}{2}\right]-1\right)$ справедливість теореми.

Теорема 3. Відстань між сусідніми точками на старшому рівні гіперповерхні і *N / 2* при парному *N* і гіперповерхні $\frac{N-1}{2}$. При нечіткому *N, N> 4*рівно $2\left(2\left[\frac{N}{2}\right]-1\right)\cdot$

Узагальнюючи розглянуте вище, отримуємо справедливість твердження

Твердження 1. Для ранжування, що описують *Ri і Rj* сусідні на старшому рівні гіперповерхні і *N / 2* при непарному *N, N> 4* справедливо

$$K_S^{Ri} \cap K_S^{Rj} \neq 0.\ \left|\overline{K_S^{Ri} \cap K_S^{Rj}}\right| = 2$$

При нечіткому *N* вони описуються однотипними розбивками.

Висновки

Результати дослідження структури гіперпростору, обраного в якості простору описів, покладені в основу створення стандартних процедури опису образів сеансових ключів і дозволило уніфікувати операції їх розпізнавання. Технічна реалізація запропонованого методу представлена в роботі [4].

Література References

[1] 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.

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

[3] V. Glushchenko, M. Petryshyn. Investigation of the space structure of session keys patterns descript Матеріали статей п'ятої Міжнародної науковопрактичної конференції "Інформаційні технології та комп'ютерна інженерія", - Івано-Франківськ. 2016. – с.113–116.

[4] В.Є. Глущенко, М.Л. Петришин Формування сеансових ключем на базі концепції прийняття рішень. Матеріали статей п'ятої Міжнародної науковопрактичної конференції "Інформаційні технології та комп'ютерна інженерія", - Івано-Франківськ. 2017. – с.252–256.