Формування Сеансовиих Ключів на Базі Концепції Прийняття Рішень

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

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

Session Keys Forming on the Base of Decision-Making Concept

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*—У статті проаналізовано застосування математичного апарату формування сеансових ключів, заснованого на концепції прийняття рішень в структурованому просторі.**

***Abstract*—The article deals with the mathematical apparatus of session keys formation based on the concept of decision-making in a structured space.**

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

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

I. Вступ

Як показують останні дослідження вітчизняних і зарубіжних авторів, одним з найбільш ефективних методів шифрування повідомлень в процесі інфообміну є методи, засновані на концепції сеансових ключів. До основних переваг алгоритмів, заснованих на даній методології, є можливість використання різних ключів для шифрування різних обсягів даних в інфопотоках повідомлень.

В ідеальному випадку необхідно забезпечити множинність та різноманітність ключів. Це зумовлює актуальність вирішення проблеми створення та застосування математичного апарату, що дозволяє формувати різноманітні сеансові ключі і забезпечує базу для створення ефективних алгоритмів роботи з такими ключами.

Мета дослідження полягає в здійсненні аналізу математичного апарату формування сеансових ключів, який базується на концепції прийняття рішень в структурованому просторі.

II. Концепція формування сеансових ключів в структурованому просторі

Концепція формування сеансових ключів в структурованому просторі полягає на наступних основних положеннях:

1. Під структурованим простором розуміється простір, що має метрику, яка дозволяє визначити віддаль між будь-якою парою точок цього простору.

2. Основним поняттям є поняття "образ ключа", під яким розуміється опис ключа за допомогою заданої системи ознак. Нехай QL^M - структурований простір з носієм A, $\|A\| = M$, де M - кількість об'єктів множини A. Множина QL - вихідна множина описів сеансових ключів $QL \in QL^M$. Описи ключів є точками простору QL^M.

3. Взаємозв'язки між точками сусідніх гіперповерхностей QA визначено відображенням $V^S \to V^{S-1}$, яке бієктивно відображає точку $y \in V^S$ на підмножину точок X_y^{S-1}, де $V^{S-1} = \bigcup_{y \in V^S} X_y^{S-1}$,

4. На множині QL визначено кластери $Q = \{Q_1, Q_2. ... Q_m\}$ множини D - допустимих описів сеансових ключів, які представлено як центри відповідних кластерів. Описи кластерів включають: описи центру, максимальної і мінімальної точок кожного кластера.

Максимальною точкою кластера Q_i, $Q_i = \{Q_1, Q_2, ..., Q_t\}$, визначено точку $R_i^M \in Q_i$, для якої справедливо $Pot\ R_i^M \geq Pot\ R_i$, $i = \overline{1, t}$, а мінімальною - точка $R_i^m \in Q_i$, $Pot\ R_i^m \leq Pot\ R_i$, $i = \overline{1, t}$. Віддаль від центру класу R_i до R_i^M визначено віддаллю до верхньої межі кластера Q_i, віддаль від R_i до R_i^m - віддаллю до нижньої межі кластера Q_i. Сукупність кластерів формують модель простору описів сеансових ключів.

5. Процес розпізнавання ключа трактується як знаходження точки погодження в моделі простору описів за множиною представлених описів. Функцією вибору точки погодження в просторі опису визначено триплет:

$$(QL,\ D \subseteq QD,\ C{:}D \rightarrow QL),$$

де QL - вихідна множина допустимих описів розпізнавання відображень $QL \in QA$, D - деяка частина множини QD всіх підмножин множини QL, $C{:}D \rightarrow QL$ - відношення, в якому для будь-якої підмножини G з QL, $D(G) \rightarrow T$, T – точка погодження. В якості точки погодження множини приймається точка T, для якої справедлива умова:

$$\bigcap_{i=1}^{n} T_i \subset T \subset \bigcup_{i=1}^{n} T_i\ .$$

III. Використання простору лінійних квазіпорядків для формування опису сеансових ключів

Розглянемо реалізацію вище наведеної концепції для формування описів сеансових ключів в просторі лінійного квазіпорядка.

Опис образів здійснюється за допомогою множини ознак A. Зв'язок між парою ознак $a, b \in A$ визначено за допомогою наступних бінарних відношень:

а) відношення еквівалентності (a–b):

$$\rho = \{(\alpha, b) : z\ (\alpha) = z\ (b)\}; \quad (1)$$

б) відношення строгого пріоритету (a, b):

$$\rho = \{(\alpha, b) : z\ (\alpha) > z\ (b)\}; \quad (2)$$

де $z\ (i)$ - значення ознаки i в заданій шкалі.

Отриманий таким чином опис способу представляє лінійний квазіпорядок у вигляді строки, що відображає впорядкування примітивів A.

Відношення еквівалентності породжує декомпозицію множини A наступним чином: α і $b \in A$ відносяться до одного класу, якщо $(\alpha, b) \subset \rho$. Такий опис способу можна подати як

$$R = \{k_1, k_2, ..., k_m\}, \quad (3)$$

$$\bigcup_{i=1}^{m} k_i = \mathrm{A}, \quad (4)$$

де k_i- клас декомпозиції A, $k_i \cap k_j = \varnothing$, $i \neq j$.

Класи декомпозиції R можна пронумерувати таким чином, що відношення ρ збігатиметься з відношенням слідування. Отримуємо, таким чином, впорядковану декомпозицію.

У випадку, коли в декомпозиції R еквівалентні елементи відсутні, тобто всі класи декомпозиції одноелементні, то відношення ρ утворює лінійний порядок.

Множини всіх відношень лінійного квазіпорядка на A з геометричної точки зору утворюють простір лінійних квазіпорядків (ПЛК), множини лінійних порядків - простір строгого порядку (ПСП).

Ранжування елементів множини A трактовано як точки цих просторів.

Для характеристики ранжування, а, отже і точок, якими вони відображаються в ПЛК, використано поняття потенціалу.

Нехай об'єкт $b \in B$ описано ранжуванням $R = \{K_1, K_2, ..., K_m\}$. Тоді для R справедливо:

$$K_S \in R \Rightarrow \left\{\forall j \neq s,\ j = \overline{1, m}, s \in [1, m] : |K_S| \geq |K_i|\right\}. \quad (5)$$

де $|K_i|$ - число елементів в класі K_i. Клас $K_S \in R$ називається класом, що визначає потенціал R, $Pot\ R = |Ki|$. Точка x, що відображає R в ПЛК, має той же потенціал, що і R. Точки потенціалу s утворюють множину V^S, розташовану на гіперповерхні U^S. ПЛК представляється у вигляді множини вкладених гіперповерхонь $QA = \bigcup_{i=2}^{N-1} U^i$, для яких:

$$\forall U^i \in QA,\ \forall i \neq j,\ i,\ i = \overline{2, N-1} \Rightarrow U^i \cap U^j = \varnothing.$$

Потенціали сусідніх гіперповерхонь відрізняються на одиницю, тобто

$$\forall U^i \in QA,\ \forall i,\ i = \overline{2, N-1} \Rightarrow Pot\ U^i - Pot\ U^{i+1}.$$

Потенціали гіперповерхонь ПЛК змінюються від 2 до $N–1$, $N = |A|$. В якості функції, що характеризує взаємне розташування точок ПЛК, використано метрику Хеммінга [3].

Позначимо через QL^M простір лінійних квазіпорядків з носієм A, $||A|| = M$, де M - кількість об'єктів множини A.

Нехай $R = \{R_1, R_2, ..., R_m\}$ і $P = \{P_1, P_2, ..., P_m\}$ – дві декомпозиції множини A. Матриці $\boldsymbol{r} = \left\| r_{i,j} \right\|^{M_{i,j}=1}$,

$\rho = \left\| \rho_{i,j} \right\|^{M_{i,j}=1}$ - матриці зв'язку елементів в декомпозиціях R і P відповідно.

Нехай

$$e_{i,j} = \begin{cases} 1, \text{якщо } (i,j) \in \rho \\ 1, \text{якщо } (i,j) \in \tilde{\rho} \\ 0, \text{якщо } (i,j) \notin \rho \end{cases} \quad (6)$$

Тоді віддаль d_x (R,P) між елементами R і P визначається за формулою:

$$d_x(R,P) = \sum_{i,j=1}^{M} \left| r_{i,j} - p_{i,j} \right|. \quad (7)$$

Отже, d_x (R,P) - кількість декомпонованих розбіжностей елементів матриць $\boldsymbol{r}$ і ρ.

Нехай сеансовий ключ b_i описується n різними образами, які належать кластеру ключа b_i. Отримані при цьому описи ключа b_i утворюють множину $W = \{R_1, R_2, ..., R_m\}$. Множина W розглядається як представлення описів зображень ключа b_i, за якими здійснюється його розпізнавання, що представляють собою процес знаходження погодженого рішення за елементами W. В якості такого рішення приймається опис, розташований між усіма елементами W. Вважається, що ранжування R знаходиться між елементами W, якщо для нього справедлива умова:

$$\bigcap_{n=1}^{n} R_i \subset R \subset \bigcup_{i=1}^{n} R_i \,. \quad (8)$$

Для знаходження погодженого рішення згідно заданого представлення W використовується апарат геометричного підходу до знаходження групового рішення [3].

Використовуючи апарат геометричного підходу до знаходження групових рішень, розроблені стандартні процедури знаходження точки погодження в ПЛК [1, 2].

При цьому досліджено властивості різних функцій вибору з урахуванням допустимих видів представлення. Показано, що функції вибору для точок $W \subseteq X_y^{S-1}$ задовольняють умову слідування, тобто $|W| > 1$, $W' \subseteq W$, $|W'| > 1$, $R \in C(W) \Rightarrow R \in C(W')$, та умову сепарування: $|W| > 1$, $W' \subseteq W$, $|W'| > 1$, $\forall W' : C(W) \Rightarrow R$, $C(W') \in C(W)$. Якщо $LW \subseteq X_{R_1}^S \bigcap X_{R_2}^S$, $|LW| > 1$, то клас функції вибору для LW має властивість узгодженості, тобто

$$\forall W, Z \subseteq LW, C(W) \bigcap C(Z) \subseteq C(W \bigcup Z) \,.$$

Отже, завдання пошуку узгоджувального рішення в ПЛК по заданому пред'явленню G в ПЛК зводиться до вибору і використання процедур знаходження точки, що задовольняє умові (8), на основі процедурних знань системи.

Таким чином, відмінна особливість запропонованого методу полягає у введенні "універсального", в певному сенсі, простору описів зображень для класифікації образів за мінімумом відстані і розробці стандартних процедур прийняття рішень на основі вхідних даних і бази знань системи.

IV. Алгоритм застосування одноразового сеансового ключа

На рис. 1 представлена схема алгоритму застосування сеансового одноразового ключа.

Першим кроком вибирається модель опису сеансових ключів, яка буде використана для вибору образу ключа, використовуваного для шифрування переданого блоку даних. Обраній моделі опису відповідає конкретне значення контрольного маркера.

На наступному кроці проводиться шифрування переданого блоку даних.

На підставі образу сеансового ключа формуються його описи, які утворюють множину представлень. Описи способу ключа генеруються випадковим чином так, щоб образ ключа був точкою погодження для точок, що утворюють множину представлень. Кількість точок множини представлень визначається рівнем секретності, який необхідно забезпечити, і якістю передачі, яку забезпечує використовувана мережа. Як показує практика, кількість точок у множині представлень не повинна перевищувати 3-4 описів [3].

Контрольний маркер і елементи множини представлень шифруються за допомогою відкритого ключа користувача. З урахуванням специфіки використовуваних алгоритмів і протоколів обміну інформацією, контрольний маркер і множина представлень можуть передаватися окремо від основних даних або бути поміщеними всередину переданого блоку інформації (пакета).

Отримувач після одержання інформації проводить дешифрування контрольного маркера і множини представлень за допомогою відкритого ключа користувача. За значенням контрольного маркера визначається модель опису образів сеансових ключів, яка використовується відправником. По точках множини представлення відновлюється образ сеансового ключа.

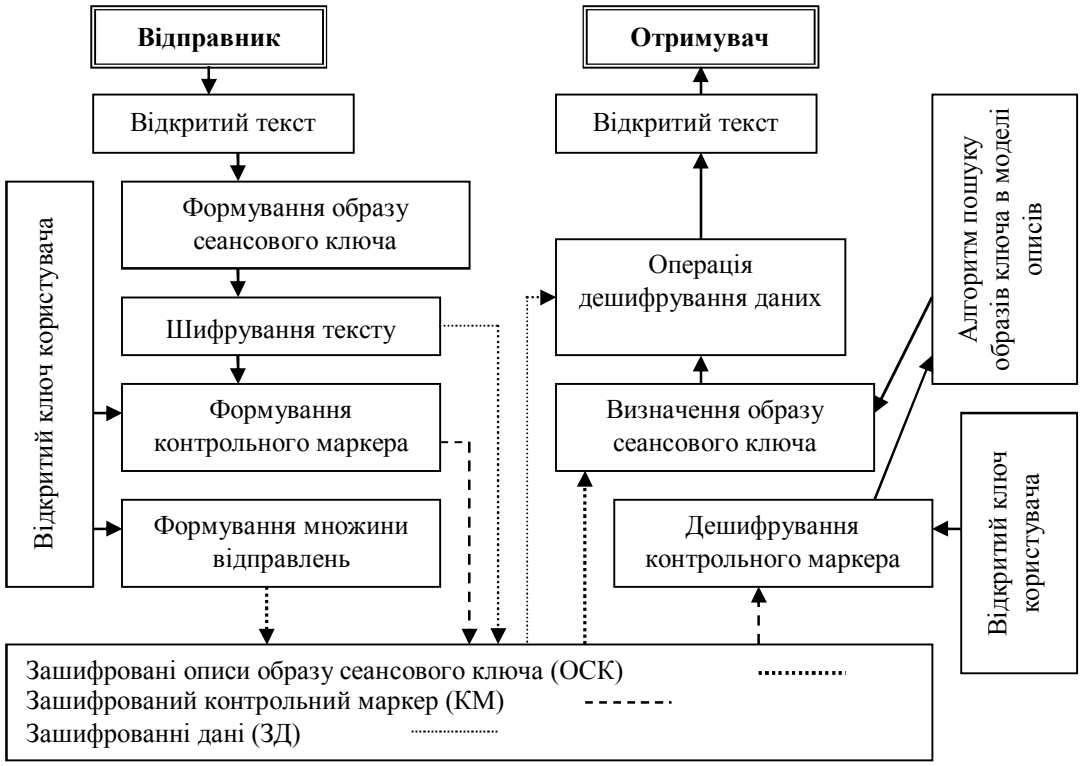

Рис. 1. Алгоритм застосування одноразового сеансового ключа.

На даному етапі автоматично вирішується завдання ідентифікація відправника.

Після визначення способу сеансового ключа проводиться дешифрування отриманих даних.

Перевагою алгоритму є те, що ключ, який використовується для шифрування повідомлень, заснований на інформації, яка є у обох користувачів, а той факт, що ключ не залежать від передачі їх один одному, забезпечує повну таємність. Сторони можуть погодити секретне значення без шифрування, і ця загальна величина може бути відразу використовуватися для шифрування даних і/або засвідчити автентичність.

V. Висновки

1. Запропонований підхід дозволяє розширити множину можливих описів сеансових ключів, і працювати з ключами нефіксованої довжини, що значно розширює продуктивність застосованого методу.

2. При формуванні сеансового ключа обидві сторони мають у своєму розпорядженні одну і ту ж інформацію про простір описів, проте операція вибору конкретного сеансового ключа базується на даних тільки однієї сторони.

3. Створення стандартних процедури опису образів сеансових ключів за моделлю описів дозволило уніфікувати операції розпізнавання образів і значно скоротити необхідний обсяг обчислень.

Література References

[1] В.Е. Глущенко, Ю.В. Глущенко, “Концептуальные вопросы построения интеллектуальных систем защиты от несанкционированного доступа,” *Вістник Східноукраїнського національного університету ім. Володимира Даля*. – 2006. – № 5 [111] – С. 48-53.

[2] V. Glushchenko, M. Petryshyn, “Investigation of the space structure of session keys patterns description” “Дослідження структури простору опису образів сеансових ключів” Матеріали Міжнародної науково-практичної конференції "*Інформаційні технології та комп’ютерне моделювання*", - Івано-Франківськ, 2016. – С. 113–116.

[3] В.Є. Глущенко, М.Л. Петришин, “Формування завадостійкого коду сеансових ключів.” Матеріали п’ятої Міжнародної науковопрактичної конференції "*Інформаційні технології та комп’ютерна інженерія*", - Івано-Франківськ. 2015. – С. 171–174.