УДК 004.056.55:004.056.53

Соловей В. А., молодший наук. співробітник
Житомирський військовий інститут ім. С. П. Корольова

КООРДИНАТНЕ КОДУВАННЯ У ДИНАМІЧНО ЕВОЛЮЦОНУЮЧИХ КРИПТОГРАФІЧНИХ ПРОСТОРАХ

У роботі розглядається концепція координатного кодування (Coordinate coding, CC) у динамічно еволюціонуючих криптографічних просторах $\mathcal{E}_t$. CC інтерпретує криптографічний процес як навігацію у внутрішньому координатному просторі GIS_t, який є компонентом $\mathcal{E}_t$. У такій моделі шифрокод є відображенням параметризованих координат деяких обраних об'єктів [1] g_i із визначеної множини. GIS_t формується двома групами об'єктів: активними $\mathcal{A}$ та пасивними $\mathcal{P}$, $\mathcal{A} \cap \mathcal{P} = \emptyset$, $|\mathcal{A}| \ll |\mathcal{PO}|$. Активні об'єкти $a_i \in \mathcal{A}$ – асоціюються із певним значенням слова відкритого тексту, тоді як пасивні об'єкти $p_i \in \mathcal{P}$ – ні. Всі об'єкти $g_i \in \mathcal{A} \cup \mathcal{P}$ динамічно переміщуються змінюючи свої координатні параметри. Простір не є статичним: він формується та трансформується [2], утворюючи послідовність унікальних конфігурацій $GIS_t = \{g_1^{(t)}, g_2^{(t)}, \dots, g_N^{(t)}\}, N = \text{const}$, $i \neq j$: $GIS_i \neq GIS_j$, $\forall t$: $|GIS_t| = N$, тому $\exists k$: $g_k^{(t+1)} \neq g_k^{(t)}$. Другим компонентом $\mathcal{E}_t$ є Логічний Тунель Часу (LTT) – це локальний контекст криптографічної обробки, що визначає правила асоціації між байтами повідомлення та об'єктами GIS, координатну систему відліку та допустимі операції векторного кодування. Функціональним стан системи $LTT_t := \langle GIS_t, R_t \rangle$,де R_t – множина правил, що визначає логічну структуру та допустимі операції у фазі t, тому: $LTT_{t+1} \neq LTT_t$. Загалом: $\mathcal{E}_t = (GIS_t, LTT_t)$ у якому кожна криптографічна подія змінює подальшу траєкторію розвитку системи.

CC реалізується трьома методами векторно-геометричного кодування (VC). Розглянемо три тригера криптографічних подій: w_1, w_2, w_3. Нехай семантика цих слів: $\mathcal{M}(w_1) = A$, $\mathcal{M}(w_2) = B$ та $\mathcal{M}(w_3) = D$. Кожне слово має своє правило асоціації $\varphi_t^1\big(\mathcal{M}(w_1)\big) = a_t^1$, $a_t^1 = A'$, $\varphi_t^2\big(\mathcal{M}(w_2)\big) = a_t^2$, $a_t^2 = B'$, $\varphi_t^3\big(\mathcal{M}(w_3)\big) = a_t^3$, $a_t^3 = D'$, тобто $A \leftrightarrow A'$, $B \leftrightarrow B', D \leftrightarrow D'$, та координати: $A' = (x_A, y_A)$, $B' = (x_B, y_B)$, $D' = (x_D, y_D)$. Перший метод (VC_1) базується на прямому кодуванні положення об'єкта A' у GIS_t. Для цього задається початок координат O та нульова вісь, після чого визначається вектор $\overrightarrow{OA'}$. Код VC_1 для слова A визначається параметрами цього вектора [2]: $c_{A'} = \big(|\overrightarrow{OA'}|, \theta_{OA'}\big)$, де $\theta_{OA'}$ - кут нахилу вектора $\overrightarrow{OA'}$. Шифрокод $c_{A'}$ формується як бінарне представлення параметризованих координат вектора $\overrightarrow{OA'}$. Реконструкція інструкції $c_{A'}$ у симетричному операційному стані однозначно знаходить $A' \Rightarrow \varphi_t^1\big(\mathcal{M}(w_1)\big) \Rightarrow A$. Другий метод ($VC_2$) базується на відносному положенні об'єкта B' відносно A'. Визначається вектор $\overrightarrow{A'B'}$, а відповідний код має вигляд як:$c_{B'} =$

$\left(\left|\overrightarrow{A'B'}\right|, \theta_{A'B'}^{\setminus B}\right)$. Метод VC_2 застосовується лише за умови верифікації попередньої події, пов'язаної з формуванням $c_{A'}$. Третій метод (VC_3) використовує визначений у фазі t базовий вектор $\overrightarrow{XY}$. Код слова D визначається як відношення параметрів вектора $\overrightarrow{B'D'}$, до параметрів базового вектора $\overrightarrow{XY}$: $c_{D'} = \left(\frac{\left|\overrightarrow{B'D'}\right|}{\left|\overrightarrow{XY}\right|}, \frac{\theta_{A'B'}^{\setminus B}}{\theta_{XY}^{\setminus D}}\right)$. Наявність базового вектора $\overrightarrow{XY}$ та верифікація події, пов'язаної з $c_{B'}$, є необхідними умовами застосування методу VC_3. У результаті формується послідовна залежність криптографічних подій (ефект храпового механізму), незалежно від джерела цих подій $w_i \in UA_t \cup NA_t$:

$$c_t = \mathcal{F}_t\left(VC_3\left(VC_2\left(VC_1\left(\mathcal{M}(w_1)\right), \mathcal{M}(w_2)\right), \mathcal{M}(w_3)\right), GIS_t, LTT_t\right),$$

де $\mathcal{F}_t$ – відображення формування шифрокоду як бінарного представлення параметрів векторної конфігурації. Після кожної операції кодування конфігурація змінюється: $GIS_{t+1} = \Psi(GIS_t, LTT_t, c_t) \Rightarrow LTT_{t+1} = \Omega(GIS_{t+1}, LTT_t, c_t)$, $\mathcal{E}_i \neq \mathcal{E}_j \Rightarrow c_i \neq c_j$. Для коректної комунікації операційні стани систем повинні залишатися симетричними. Тільки верифіковані події c_i опосередковано впливають на траєкторію еволюції системи. Верифікація шифрокоду описується: $V_{\mathcal{E}_t}(c_t) \in \{0,1\}$. Успішна верифікація: $V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow g_i \in \mathcal{A}_t$, $G(c_t) \subset \mathcal{A}_t$, де $G(c_t) = \{g_{i_1}, \dots, g_{i_k}\}$ – підмножина об'єктів індукована c_t. Верифіковані події є тотожними, траєкторія еволюції симетрична: $\forall t \in N: \mathcal{E}_t^{Alice} = \mathcal{E}_t^{Bob}$.

Таким чином безпека визначається динамікою внутрішнього стану системи, а не секретністю чи складністю криптографічних ключів: $Security = f(GIS_t, LTT_t)$. Тому конфіденційність виникає як наслідок унікальності GIS; автентифікація – як властивість симетричної узгодженості LTT; цілісність – як результат координатної залежності w_i (g_i) криптографічних подій: $w_{i+1} = VC_{i+1}(w_i)$ та $V_{\mathcal{E}_t}(c_t) = 1$.

У такій моделі криптографічна стійкість виникає як властивість еволюції системи, а не як наслідок секретності ключового простору: $Security \not\subseteq KeySpace,\ KeySpace = \emptyset$. Отже СС слід розглядати не як окремий алгоритм, а як криптографічну модель, у якій криптографічні властивості виникають як наслідок еволюції внутрішнього координатного простору системи. Процес шифрування не зводиться до фіксованого відображення, а визначається динамікою стану, що формує онтологічно замкнений та метаданонейтральний канал зв'язку: $Enc(m,k) \not\equiv F(m, GIS_t, LTT_t)$. Шифрокод не має глобального значення. Його інтерпретація можлива лише у власному фазовому просторі: $Decode_{\mathcal{E}}(c_t) = g_t \Leftrightarrow \mathcal{E} = \mathcal{E}_t$.

Список використаних джерел

1. Conway J. H., Sloane N. J. A. Sphere Packings, Lattices and Groups. – Springer, 1999.

2. Cover T. M., Thomas J. A. Elements of Information Theory. – Wiley, 2006.