УДК 004.056.55:004.056.53

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

ПАРАДИГМА ФОРМУВАННЯ ЕКСПОНЕНЦІЙНО СТІЙКИХ ШИФРОКОДІВ У КООРДИНАТНІЙ КРИПТОГРАФІЇ

У роботі розглядається парадигма формування експоненційно стійких шифрокодів (c) у межах Координатної Криптографічної моделі (КК). У класичних криптографічних системах шифротекст є результатом криптографічного перетворення відкритого тексту (w) за допомогою алгоритму та секретного ключа. Шифрокод c_t у КК не містить криптографічно перетвореного тексту, а виступає навігаційною інструкцією, реконструкція якої дозволяє знайти об'єкт g_i у віртуальному просторі. Будь-якої іншої семантики, крім необхідної для реконструкції координатної події – c_t не містить. Знайдений об'єкт належить до визначеної множини, яка за кількістю біт повному алфавіту одного слова тексту. Кількість біт w (алфавіт) система визначає сама. Кожне w, за номером w_1, w_2, … w_n має свою окрему асоційовану множину та унікальне правило асоціації. Якщо хоч одне w_n було відновлено за допомогою одного g_i визначеної множини – правило асоціації нівелюється та всі g_i цієї множини змінюють свої координати.

Криптографічний стан системи визначається як $\mathcal{E}_t = (GIS_t, LTT_t)$, де GIS_t – геометричний координатний стан внутрішнього простору системи у фазі t, а LTT_t – логічний тунель часу, що визначає функціональний контекст системи у цій фазі. $\mathcal{E}_t$ визначає правила формування та реконструкції шифрокоду: $c_t = F_{\mathcal{E}_t}(w_t)$, де $F_{\mathcal{E}_t}$ – унікальна композиція перетворень, що визначається унікальним поточним станом системи. Реконструкція w_t відбувається у два етапи: $c_t \to G_t(c_t) \to w_t$, де $G_t(c_t)$ – множина координатних подій реконструкції g_i внутрішнього простору. GIS_t складається з активної та пасивної множини об'єктів: $A_t \cap P_t = \emptyset$,

$GIS_t = A_t \cup P_t$, принципова умова: $|A_t| \ll |P_t|$. Для слова довжини m біт множина можливих значень: $|W| = 2^m$, тому для кожного слова, незалежно від його значення система резервує $A_t^i \subset A_t : |A_t^i| = 2^m$. Правило асоціації бієктивне: $\varphi_t^i: W \to A_t^i$, активний об'єкт a_i має суперпозиційне координатне представлення: $\Sigma_t(o_t) = \{v_t^{(1)}, v_t^{(2)}, \dots, v_t^{(r)}\}$. Суперпозиція координат є властивістю простору, а не повідомлення. Розв'язання суперпозиції визначається відображенням $\psi_t: \Sigma_t(o_t) \to \{v_t^*\}$.

Координатні параметри v_t^* використовуються для формування бінарного представлення події. Надалі виконується композиція криптографічних перетворень: перестановки, дифузія, XOR-операції тощо. Реконструкція шифрокоду, така, що всі k знайдені об'єкти належать тільки до A_t – та будуть вірно відновлені всі слова тексту – можлива тільки за умови симетрії $\mathcal{E}_t$ у поточній фазі та симетричної

еволюції: $\mathcal{E}_{t+1}^{Alice} = \mathcal{E}_{t+1}^{Bob}$. Шифрокод – це подія, яка не має ніякої семантики окрім навігаційної.

Симетричну еволюцію $\mathcal{E}_t$ забезпечує механізм логічної безпарольної автентифікації (LPA), який через логічний висновок встановлює систему автора – через механізм верифікації отриманого від нього шифрокоду.

Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом, який верифікується як «свій» (інакше – «чужий») тоді і тільки тоді, коли виконується предикат верифікації:

$$V_{\mathcal{E}_t}(c_t) \in \{0,1\}, \quad V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t,$$

де $V_{\mathcal{E}_t}$ – функція LPA, а значення 1 відповідає прийняттю («свій»). LPA не потребує знання семантики відкритого тексту і базується виключно на логічній узгодженості структури шифрокоду з параметрами фазової симетрії системи. c_t може бути верифікований лише системами з симетричним операційним станом: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow V_{S_t}(c) = 1,\ accept$, що дозволяє зробити логічний висновок про автора шифрокоду.

Визначимо простір всіх можливих операційних криптографічних станів системи: $\mathcal{S} = \{(GIS_t, LTT_t)\}$. Для будь-якого W та будь-якого c_t існує криптографічний стан системи, у якому цей шифрокод може бути згенерований: $\forall w \in W,\ \forall c \in C\ \exists \mathcal{E}_t$: $c = F_{\mathcal{E}_t}(w)$.

У теорії інформації абсолютна криптостійкість досягається у шифрі C одноразового блокнота OTP, визначається: $I(W;C) = 0$.

Якщо $LTT_t = \Phi_t(c_{t-1}, c_{t-2}, \dots) \Rightarrow |LTT| \sim 2^t$, тоді $|S| = |GIS| \cdot |LTT|$ та $|S| \approx |GIS_t|! \cdot |C|^t$потужність простору значно перевищує простір ключів OTP: $|\ K_{OTP}\ | = 2^{|W|} \Rightarrow |S| \gg |K_{OTP}|$.

Оскільки шифрокод C, сформований в межах моделі координатної криптографії - не містить семантики відкритого тексту W, тому взаємна інформація $I(W;C) = 0$ – для зовнішнього спостерігача.

Простір ключів OTP є частковим випадком простору криптографічних станів системи $|S| \gg |K_{OTP}| \rightarrow \boxed{K_{OTP} \subset S}$.

У Координатній криптографії абсолютна криптостійкість виникає як властивість простору операційних криптографічних станів системи. Цю властивість можна інтерпретувати як стан-підсилену абсолютну секретність (state-amplified secrecy). Надійність систем безпеки, що сформовані у межах моделі КК полягає у тому, що у Shannon-моделі: $\forall m, c\ \exists k$ – потрібен ключ, цій системі: $\forall w, c\ \exists \mathcal{E}_t$ – ключ не потрібен.

Таким чином КК формує новий клас шифрокодів у яких криптографічна стійкість виникає як властивість немарковської стохастичної еволюції криптографічного стану системи шифрування.

Список використаних джерел

1. Bellare M., Pointcheval D., Rogaway P. Authenticated key exchange secure against dictionary attacks // EUROCRYPT. – 2000.

2. Shannon C. A mathematical theory of communication // Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423.