УДК 004.056.55:004.056.53

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

ЕВОЛЮЦІЙНІ ІМПЛІЦИТНІ КАНАЛИ ПЕРЕДАЧІ ІНФОРМАЦІЇ У КООРДИНАТНІЙ КРИПТОГРАФІЇ

У роботі розглядається новий клас каналів передачі інформації, що виникає у межах криптографічної парадигми координатної криптографії (КК) – еволюційні імпліцитні канали. На відміну від традиційних криптографічних систем, у яких передача інформації здійснюється виключно через явно визначені бітові структури шифротексту, у КК можлива передача додаткової інформації через структурні властивості відхилень [1], що виникають у процесі верифікації кожного шифрокоду – логічної безпарольної автентифікації (LPA). Такі канали не є окремими протоколами поверх криптосистеми, а виникають як природна властивість внутрішньої математично-геометричної структури координатної криптографії. Формування шифрокоду описується відображенням $c_t = F(m_t, n_t, \mathcal{E}_t)$, де $\mathcal{E}_t$ – операційний стан системи у фазі t, m_t – компонент відкритого тексту, n_t – вектор імітаційних даних, F – координатне відображення формування шифрокоду. Кожна подія формування шифрокоду впливає на фазову еволюцію системи: $\mathcal{E}_{t+1} = \Psi(S_t, c_t)$, де Ψ – фазово-залежне стохастичне відображення. Отриманий шифрокод підлягає процедурі LPA, оскільки тільки верифікована подія впливає на еволюцію системи $\mathcal{E}_{t+1}$. Координатний простір GIS_t є компонентом $\mathcal{E}_t$, формується з об'єднання активної $\mathcal{A}_t$ та пасивної $\mathcal{P}_t$ множин об'єктів: $\mathcal{A}_t \cap \mathcal{P}_t = \emptyset$, $GIS_t = \mathcal{A}_t \cup \mathcal{P}_t$, при цьому обов'язково: $|\mathcal{A}_t| \ll |\mathcal{P}_t|$. Кожен об'єкт $g_i \in \mathcal{A}_t \cup \mathcal{P}_t$ має унікальні координатні параметри. Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом, c_t приймається тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0,1\}$, $V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція LPA, а значення 1 відповідає прийняттю. Однак у випадку результату $V_{\mathcal{E}_t}(c_i) = 0 \rightarrow$ reject LPA не одразу відхиляє шифрокод, а формує структуру відхилення $E(c_t)$, що відображає відмінність координатних параметрів від очікуваних. У традиційних криптографічних системах подібне відхилення інтерпретується як модифіковене повідомлення. Проте у КК множина відхилень може мати структуровану форму, формально: $E(c_t) = \{e_1, e_2, \dots, e_n\}$, де e_k – відхилення координатного параметра k-го слова від очікуваного значення. Якщо структура відхилень відповідає певному еволюційному правилу R_t, то така подія інтерпретується як імпліцитний сигнал $M_t^{(imp)}$ відповідно до фазового правила інтерпретації відхилень IC_t: $E(c_t) \in R_t \Rightarrow implicit_{message}$, $IC_t: E(c_t) \rightarrow M_t^{(imp)}$. Оскільки $|\mathcal{A}_t| \ll |\mathcal{P}_t|$, у моделі КК виникає неявний канал,

індукований структурою відхилень при відхиленні шифрокоду: $V_{\mathcal{E}_t}(c_t) = 0 \Rightarrow E(c_t) = \{e_1, \dots, e_n\}$.

Оскільки $R_t = f(H_t)$, де H_t – подієва пам'ять обмеженої фазової глибини, стан якої змінюється після кожної події $V_{S_t}(c_i) = 1$, то імпліцитний канал (ІК) не має сталої параметризації та не є бітовим [1]. Таким чином правила інтерпретації структурованих відхилень не задаються наперед, а еволюціонують разом із системою. Унаслідок цього формується ІК передачі інформації, як математичний додатковий шар комунікації: $C_{total} = C_{pr} \cup C_{im}$, де C_{pr} – основний канал передачі відкритого тексту, а C_{im} – додатковий ІК передачі інформації через структуровані відхилення. ІК не впливає на пропускну здатність основного каналу – інформація передається через попередньо сформовані R_t, тому ІК не потребує додаткових бітів у шифрокоді. Загальна інформаційна місткість системи подається як [2]:

$$Capacity(C_{total}) = Capacity(C_{pr}) + Capacity(C_{im}).$$

Ймовірність випадкового виникнення структурованої помилки у модифікованому шифрокоді, що відповідає поточному правилу R_t, є надзвичайно малою та задається наперед параметрами безпеки ІК. Якщо припустити, що координатні параметри мають множину можливих значень N, то ймовірність випадкового виконання складного правила оцінюється як $Pr(E(c_t) \in R_t) \approx N^{-k}$, де k – кількість координатних елементів, що беруть участь у правилі. У практичних системах це значення прямує до нуля, тому ІК дозволяють реалізувати додатковий рівень передачі інформації, який не порушує властивостей метаданонейтральності основного каналу та не змінює структуру криптографічного процесу. ІК передають інформацію через структурні властивості координатних відхилень шифрокоду. Такі канали можуть бути визначені як еволюційні імпліцитні канали – новий клас каналів у теорії інформації: Ch_{eIC} (evolutionary implicit channels). Інформація не передається через безпосередні бітові значення шифрокоду, тому:

$$I_{struct} = I(E(c_t); R_t),\ I_{total} = I(C_{primary}) + I(E(c_t); R_t).$$

Декодування: $Decode(c_t) = \left(D_{primary}(c_t),\ D_{implicit}(E(c_t))\right)$, де $D_{primary}$ – декодування основного повідомлення, а $D_{implicit}$ – інтерпретація структури відхилень координатних параметрів. Таким чином один шифрокод може одночасно переносити два незалежні інформаційні повідомлення. Якщо c_t містить n координатних слів, а кожне слово має k допустимих варіантів відхилення, то кількість можливих структур сигналу становить $|E(c_t)| = k^n$. Таким чином простір потенційних каналів Ch_{eIC} у координатній криптографії має експоненційну потужність.

Список використаних джерел

1. Simmons G. J. The prisoners' problem and the subliminal channel // *CRYPTO*. – 1983. – P. 51–67.

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