УДК 681.327.11

Н. В. Сачанюк-Кавецька
Вінницький Національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Кодування як засіб захисту інформації у системах контролю доступу з використанням логіко-часових функцій у формі поліномів і біометричних даних суб'єктів

Розглянуто можливість циклічного кодування та правила побудови ключів асиметричного криптоалгоритму на базі ідентифікаційних логіко-часових функцій, що містять усі важливі характеристики переданих повідомлень. Для доступного формального опису такого кодування та правил побудови ключів використано подання логіко-часових функцій у формі поліномів.

Ключові слова:*логіко-часова функція, Δ-інтервал, поліном, циклічний код, ключ.*

Вступ

Бурхливий розвиток інформаційних технологій призвів до зростання відносної важливості окремих аспектів суспільного життя, зокрема, будь-якої інформації. Інформація має певну цінність (може продаватись), вона не локалізована в просторі та може легко поширюватись. Інформація існує у різних формах: її можна зберігати на комп'ютерах, передавати обчислювальними мережами, роздруковувати або записувати на папері, а також озвучувати у розмовах. З погляду безпеки всі види інформації потребують надійного захисту. Використання комп'ютерних систем і мереж для вирішення різноманітних підприємницьких завдань, стратегічного розвитку, реалізації різноманітних зв'язків підприємств з їх партнерами, клієнтами, керуючими установами в on-line режимі дало можливість не обмежувати інформаційні потоки та інформаційні процеси межами окремого підприємства. Інформація та інформаційні системи, мережі, в яких функціонують підприємства, організації, установи, є їхніми надзвичайно важливими ресурсами [1]. Саме доступність, цілісність та конфіденційність інформації може мати особливе значення для конкурентоспроможності та репутації організації, її рентабельності, відповідності управлінських рішень правовим нормам законодавства України та міжнародним правовим вимогам. З іншого боку, з кожним днем з'являються нові загрози, які здатні нанести збитки організації. Це, наприклад, хакерські дії, соціальна інженерія, втручання до системи, злом, несанкціонований доступ до системи,

комп'ютерні злочини, продаж інформації, атаки на систему, перегляд інформації з обмеженим доступом, фальсифікація та підроблення даних, зловмисні коди, продаж інформації тощо. Водночас, унаслідок посилення залежності організацій від інформаційних, комунікаційних систем і послуг вони можуть стати вразливішими до порушень режиму безпеки. Захисні заходи є ефективнішими, якщо вони вбудовані в інформаційні системи та послуги на етапах формування технічного завдання та проектування. Чим швидше організація запроваджує заходи із захисту своїх інформаційних і комунікаційних систем, тим ефективнішими та дешевшими вони будуть у майбутньому. Одним із основних невід'ємних елементів комплексної системи інформаційної безпеки є підсистема управління доступом до інформаційних ресурсів. Віднедавна, дедалі більше уваги привертає біометрія, як одна з новітніх інформаційних технологій, в якій використовуються унікальні характеристики об'єктів ідентифікації і веріфікації. Тому актуальним є питання захисту інформаційних ресурсів від несанкціонованих управлінських дій і доступу сторонніх осіб або програм до комп'ютерних даних.

Огляд проблем і постановка задачі створення засобів захисту інформації у системах контролю доступу з використанням унікальних характеристик об'єктів

З появою та розвитком інформаційних технологій актуальною стала проблема інформаційної безпеки, яка пов'язана зі збереженням конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах. Зовнішнім впливам зазвичай протидіють за допомогою різноманітних програмно-технічних методів захисту. Сутність методів захисних перетворень полягає в тому, що інформація, яка зберігається у системі та передається каналами зв'язку, перетворюється на шифрограму, тобто в закритий (кодований) текст або графічне зображення документа [2]. У такому вигляді повідомлення передається навіть не захищеним каналом зв'язку. Санкціонований користувач після отримання повідомлення дешифрує його за допомогою зворотного перетворення (ключа), внаслідок чого виходить вихідний, відкритий вид переданого повідомлення. Кодування, окрім цілей захисту, дає змогу підвищити швидкість доступу до даних. В основу шифрування покладено два елементи: криптографічний алгоритм і ключ [3, 4]. Загальні криптоалгоритми часто стають стандартами шифрування, якщо доведено їхню високу криптостійкість. Криптостійкість загальних алгоритмів визначається довжиною ключа шифрування, який генерується методом випадкових чисел і не може бути повторений протягом тривалого часу. Є дві великі групи загальних криптоалгоритмів: симетричні та асиметричні. До симетричних алгоритмів належать такі, в яких шифрування та дешифрування виконується однаковим ключем, та які мають досить високу швидкість обробки як для апаратної, так і для програмної реалізації. Основним їхнім недоліком є труднощі, що пов'язані з дотриманням безпечного розподілу ключів між абонентами системи. Для асиметричних алгоритмів, шифрування та дешифрування виконують за допомогою різних ключів. Такі алгоритми потребують значно довшого часу для обчислення, але не створюють труднощів під час розподілу ключів. Найбільш переспективними системами захисту даних сьогодні вважаються саме асиметричні системи з відкритим ключем. Можна

стверджувати, що для шифрування з метою передачі інформації використовують асиметричні алгоритми, а для шифрування з метою зберігання інформації — симетричні.

Останні десятиліття велика увага науковців у галузі інформаційної безпеки приділяється біометриці [5] як формі управління ідентифікаторами доступу та контролю доступу. Як самостійна наука, біометрія виникла в кінці 19-го століття в роботах Ф. Гальтона, який зробив великий внесок у створення кореляційного та регресійного аналізу, та К. Пірсона — засновника найбільшої біометричної школи. Біометричні системи можуть працювати в двох режимах: веріфікації, завдання якої звірити відповідність вимірюваної біометричної характеристики записаному шаблону заявленого індивідуума, та ідентифікації, при якій вимірюється біометрична характеристика, що буде порівнюватися з базою раніше записаних шаблонів усіх «відомих» об'єктів.

Біометричні дані можна розподілити на два основні класи:

— статистичні, які ґрунтуються на фізіологічних унікальних характеристиках об'єктів (за відбитком пальця, за термограмою обличчя, за формою долоні, за сітківкою ока, за ДНК, за розташуванням вен на лицьовій стороні долоні і т. ін), що практично не змінюються з часом;

— динамічні, які ґрунтуються на поведінковій характеристиці суб'єктів, тобто побудовані на особливостях, які характерні для підсвідомих рухів у процесі відтворення якої-небудь дії (за почерком, за клавіатурним почерком, за голосом тощо).

Усі перераховані підходи захисту інформації досить легко реалізувати в логіко-часовому середовищі, перетворивши всі параметри необхідного для передачі повідомлення на логіко-часові функції (ЛЧФ) [6], яких є три функціонально повні класи. Наприклад, елементарна ЛЧФ першого класу, що між двома нулями приймає стале значення:

$$f(t,t_1,T_1)=\begin{cases} t-t_1, & якщо \quad t_1 < t \le t_1+T_1, \\ 0, & якщо \quad t_1+T_1 < t \le t_1 \end{cases}$$

де t — поточне значення параметра часу; t_1 — часова координата; T_1 — тривалість відрізку існування.

ЛЧФ розглядаються на часовому проміжку $[t_k, t_{k+1}]$, дискретизованому за допомогою Δ-інтервалу (Δ-дискретизації) — мінімального часового інтервалу, довжиною Δ_i ($\Delta_i = t_{i+1} - (t_i + T_i)$), між двома часовими координатами ЛЧФ. Надалі, для простоти викладення матеріалу, ЛЧФ будемо позначати $f_i(t)$. ЛЧФ біометричні характеристики об'єктів ранжують за мірою важливості, а на основі синтезованих ознак формують ідентифікаційну ЛЧФ (фактично шифровані дані) [7], яка є унікальною для даного об'єкта. Ідентифікують об'єкт шляхом порівняння отриманої ідентифікаційної функції з еталонними зразками бази знань. За умови неповної ідентифікації здійснюється розширення бази знань шляхом запису отриманого результату порівняння в пам'ять як нового зразка та визначення найбільш близького до отриманого еталонного зразка.

Метою даної статті є розробка можливого варіанту циклічних кодів у логіко-часовому середовищі та правила побудови ключів асиметричного криптоалгоритму на базі ідентифікаційної ЛЧФ.

Основні положення

Система кодування інформації є одним із ключових моментів розробки політики інформаційної безпеки та значно підвищує захист інформаційної інфраструктури від несанкціонованого доступу. Для спрощення обрахунків у логіко-часовому середовищі можна використати циклічні коди, оскільки це є ціле сімейство завадостійких лінійних кодів, що забезпечують досить велику гнучкість з точки зору можливості реалізації коду з необхідною здатністю виявлення та виправлення помилок. Циклічний код відноситься до систематичних блочних (n, k) кодів, у яких k перших розрядів є комбінацією первинного коду, а наступні $(n-k)$ розрядів є перевірними.

В основі побудови циклічних кодів лежить операція ділення заданої ЛЧФ на породжуючий незвідний поліном ступеня r. Остача від ділення використовується при формуванні перевірних розрядів. При цьому операції ділення передує операція множення, яка здійснює зсув вліво k-розрядної інформаційної кодової комбінації на r розрядів.

На довільному Δ-інтервалі розбиття ЛЧФ може змінювати своє значення. В таких випадках доцільно коригувати значення відповідної функції. Це коригування ідентичне квантуванню, але для ЛЧФ таке коригування виконується за тією ж координатою, що й дискретизація. У цьому контексті краще використати термін «фільтрація». Тобто, для математичного опису повідомлення використовуються фільтровані функції.

Опис циклічних кодів і їхню побудову зручно проводити за допомогою многочленів (або поліномів) [8]. Слід відмітити, що запис ЛЧФ у вигляді поліномів дозволяє відобразити формалізованим чином операцію циклічного зсуву вихідної ЛЧФ. Наприклад, для ЛЧФ другого класу, яка містить два відрізки існування, що не перетинаються між собою (рис. 1), відповідає поліном: $P_6(t) = t^2 + t^3 + t^6$, а монотонно зростаючій ЛЧФ, що зображена на рис. 2, відповідає поліном: $P_2(t) = t + 2t^2$.

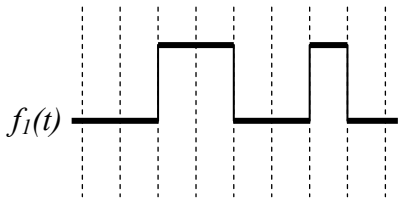

Рис. 1. Можливий варіант ЛЧФ з двома відрізками існування

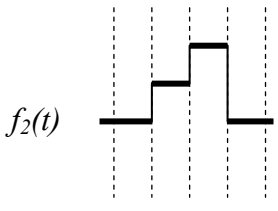

Рис. 2. Можливий варіант зростаючої ЛЧФ

Для представлення вихідного повідомлення, переданого у вигляді ЛЧФ, циклічним кодом, дотримуються наступного алгоритму.

1. Подаємо вихідне повідомлення (ЛЧФ) у вигляді поліному $P_r(t)$.

2. Визначаємо контрольне число Δ-інтервалів (r — порядок поліному повідомлення). Визначаємо відповідно контрольному числу породжуючий поліном $P(t)$.

3. Домножуємо $P_r(t)$ на t^r.

4. Ділимо $P_r(t)\cdot t^r$ на породжуючий поліном. Остачу такого ділення позначаємо через $R(t)$.

5. Формуємо поліном кодованого повідомлення $A(t)=P_r(t)\cdot t^r+R(t)$ та будуємо відповідну йому ЛЧФ.

Слід зауважити, що кодоване повідомлення немає помилок (інформація передана правильно), якщо остача від ділення цього повідомлення на породжуючий поліном дорівнює нулю. Операція ділення є звичайним діленням многочленів, однак замість віднімання використовуємо операцію нерівнозначного віднімання ($|k|$), яка базується на Δ-дискретизації:

$$f_1(t,t_{11},T_{11},a_1)\,|k|\,f_2(t,t_{21},T_{21},a_2)=\left\{(t-(t_1+i\Delta_i))\cdot|a_{i1}-a_{i2}|,\ t_1=\min(t_{11},t_{21})\right\},$$

де

t_{11}, t_{21} — часові координати змінних;

T_{11} та T_{21} — тривалості відрізків існування першої та другої функції;

a_1 та a_2 — відповідні амплітуди;

i — кількість Δ- інтервалів в обраному часовому інтервалі;

Δ_i — тривалість Δ-інтервалу;

a_{i1}, a_{i2} — відповідні амплітуди на i-му Δ-інтервалі.

Результатом цієї операції буде знову ЛЧФ, яку можна назвати нерівнозначною різницею.

Знайдемо кодоване повідомлення для поліному $P_6(t)=t^2+t^3+t^6$. У даному випадку контрольне число Δ-інтервалів $r=6$, тому $P(t)=t^6+t+1$ — породжуючий поліном. Помножимо поліном переданого повідомлення на t^6: $P_6(t)\cdot t^6=t^8+t^9+t^{12}$. Остача від ділення одержаного поліному та породжуючий буде $R(t)=t^4+1$. Таким чином, поліном кодованого повідомлення $A(t)=P_r(t)\cdot t^r+R(t)=t^{12}+t^9+t^8+t^4+1$. ЛЧФ, що відповідає даному поліному подано на рис. 3.

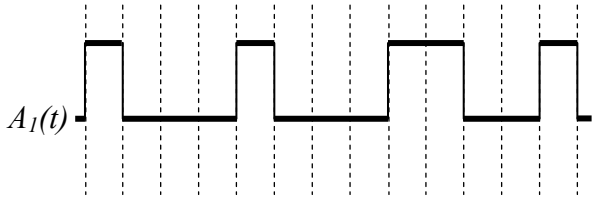

Рис. 3. Кодоване повідомлення інформації, переданої ЛЧФ $f_1(t)$

Оскільки частка від ділення кодованого повідомлення на породжуючий поліном дорівнює нулю, то дане повідомлення не містить помилок.

Знайдемо кодоване повідомлення для зростаючої ЛЧФ $f_2(t)$, зображеної на рис. 2. Даній функції відповідає поліном $P_2(t) = t + 2t^2$ з контрольним числом $r = 2$. Таким чином, породжуючий поліном набуває вигляду $P(t) = t^2 + t + 1$ і $P_2(t) \cdot t^6 = 2t^4 + t^3$. Виконавши ділення одержаного поліному на породжуючий, одержуємо $R(t) = 2t + 2$. Отже, $A(t) = P_r(t) \cdot t^r + R(t) = 2t^4 + t^3 + 2t + 2$ і ЛЧФ, що відповідає даному поліному, зображена на рис. 4.

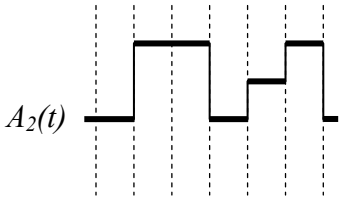

Рис. 4. Кодоване повідомлення інформації, переданої зростаючою ЛЧФ $f_2(t)$

Так як $\dfrac{2t^4 + t^3 + 2t + 2}{t^2 + t + 1} = 2t^2 + 2$ і залишок дорівнює нулю, то дане повідомлення не містить помилок.

Для кращого приховування інформації та її захисту від модифікації, підробки або викривлення можна використовувати асиметричні алгоритми, які дозволяють виконувати шифрування в різних режимах.

1. За допомогою таємного ключа відправника. Тоді всі, хто має відкритий ключ, можуть розшифрувати передане повідомлення.

2. Шифрування за допомогою відкритого ключа отримувача, тоді тільки власник таємного ключа, який є парним до цього відкритого, може розшифрувати таке повідомлення.

3. За допомогою таємного ключа відправника і відкритого ключа отримувача переданого повідомлення. Тоді тільки потрібний отримувач може розшифрувати таке повідомлення.

Оскільки не існує двох людей з однаковим біометричними характеристиками, то доцільно саме їх використовувати при побудові ключів шифрування та дешифрування. Більше того, в ідентифікаційній ЛЧФ можна використовувати декілька характеристик, ранжованих за важливістю. Оскільки при виділенні ознак використовується похідна ЛЧФ, яка виділяє контури зображень, то при побудові ЛЧФ-ключа доцільно використовувати такі 5 характеристик (від кращих до гірших): райдужна оболонка ока, відбиток пальця, форма долоні, розміщення вен на долоні, форма обличчя. Причому, ключ відправника може містити його біометричні характеристики, а ключ для розшифровування повідомлення — характеристики отримувача.

При побудові ключів криптоалгоритмів із використанням біометричних характеристик необхідно дотримуватися таких правил.

1. Для кожної біометричної характеристики будуємо ЛЧФ з використанням операції диференціювання [6]:

$$f(t_1,...,t_m,T_1,...,T_m,a_1,...,a_m),$$

де $t_1,...,t_m$ — часові координати; $T_1,...,T_m$ — відповідні відрізки існування; $a_1,...,a_m$ — амплітуди, що відповідають даним відрізкам існування.

Зауважимо, що найкраща характеристика має амплітуду $a=5$, а найгірша — $a=1$.

2. Одержуємо ЛЧФ-ключ як результат нерівнозначного віднімання одержаних у попередньому пункті функцій.

3. Записуємо ЛЧФ-ключ у вигляді полінома, де коефіцієнт біля відповідного ступеня змінної t дорівнює значенню відповідної амплітуди a_i. Зауважимо, що даний ключ можна подати не тільки у вигляді полінома, а і як матрицю амплітуд розмірністю $1\times m$.

Висновки

Спосіб циклічного кодування ідентифікаційних ЛЧФ, що містять усі важливі характеристики переданого повідомлення, значно підвищує захист інформаційної інфраструктури від несанкціонованого доступу. Використання логіко-часового середовища дозволяє передати велику кількість інформації з мінімальною кількістю помилок. Запропонований спосіб циклічного кодування досить легко апаратно реалізувати на базі регістрів зсуву з прямими та зворотними зв'язками.

Головне досягнення асиметричного шифрування полягає в тому, що воно дозволяє людям, які не мають домовленості про безпеку, обмінюватись секретними повідомленнями. Унікальність ключів з біометричними характеристиками на базі ідентифікаційних ЛЧФ полягає у неможливості відновлення та читання повідомлення несанкціонованим користувачем, швидкому реагуванні на атаки та достатньо малому часі шифрування та дешифрування. Більше того, користувач-зловмисник не може видати себе за відповідного абонента. Використання таких ключів зводить можливість порушення конфіденційності до мінімуму. Ключі з біометричними характеристиками на базі ідентифікаційних ЛЧФ можуть бути використані для підтвердження авторства та мають просту процедуру обміну та просте математичне дослідження, оскільки вони подаються у вигляді поліномів. Можна стверджувати, що досить легко керувати такими ключами у великій мережі.

1. Смит С. Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников; пер. с англ. А.Ю. Линовича, С.В. Витязева, И.С. Гусинского. Москва: Додэка XXI, 2012. 720 с

2. Панасенко С.П. Алгоритмы шифрования: специальный справочник. Санкт-Петербург, 2009. 230 с.

3. Русин Б.П., Варецький Я.Ю. Біометрична аутентифікація та криптографічний захист. Львів: Коло, 2010. 287 с.

4. Ахрамович В.М. Ідентифікація й аутентифікація, керування доступом. *Сучас. захист інформації*. 2016. № 4. С. 47–51.

5. Гнідець Т.Я. Біометрія: сильні та слабкі сторони. *Науковий вісник Львівського державного університету внутрішніх справ*. 2014. № 2. С. 273–282.

6. Сачанюк-Кавецька Н.В., Кожем'яко В.П. Елементи око-процесорної обробки зображень у логіко-часовому середовищі. Монографія. Університет-Вінниця, 2004. 135 с.

7. Сачанюк-Кавецька Н.В. Визначення чутливості ідентифікаційної функції до зміни вхідних характеристик обробки зображень для розпізнавання суб'єктів у системах захисту інформації. *Реєстрація, зберігання і оброб. даних.* 2017. Т. 19. № 1.С. 55–64.

8. Sachaniuk-Kavets'ka N., Kozhemiako V., Wojcik W., Kassymkhanova D., Kalizhnova A. The use polynomials as a possible variant analytical processing on logic-time functions. *Optical Fibers and Their Applications 2015 Proceedings of SPIE*. Vol. 9816. Lublin, Poland. 98161S-1 to 98161S-2.

Надійшла до редакції