V Висновки

Вперше застосована на практиці імовірнісна алгебраїчна атака. Об'єкт атаки - потоковий шифратор «SFINKS» з послабленою фільтруючою функцією. Були написані дві програми – для реалізація шифратора та для його криптоаналізу. Програма криптоаналізу успішно знаходить ключ. Цим доведено, що імовірнісна алгебраїчна атака може бути втілена на практиці.

Оскільки функції, вразливі до імовірнісних алгебраїчних атак, можуть мати дуже хороші всі інші криптографічні властивості, то потокові шифратори, які не розроблялися стійкими проти алгебраїчних атак (зокрема розроблені до 2003), можуть виявитися вразливими до імовірнісної алгебраїчної атаки.

Література: ***1.*** *An Braeken, Joseph Lano, Nele Mentens, Bart Preneel and Ingrid Verbauwhede. Sfinks specification and source code // April 2005, Available on ECRYPT Stream Cipher Project page, http://www.ecrypt.eu.org/stream/sfinks.html* ***2.*** *Nicolas Courtois and Willi Meier. Agebraic Attacks on Stream Ciphers with Linear Feedback // Eurocrypt 2003, Warsaw, Poland, LNCS 2656, pp. 345–359, Springer. An extended version is available at http://www.minrank.org/toyolili.pdf* ***3.*** *Nicolas Courtois. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback // Crypto 2003, LNCS 2729, pp: 177-194, Springer.* ***4.*** *Nicolas Courtois. Algebraic Attacks on Combiners with Memory and Several Outputs // ICISC 2004, LNCS, to appear in Springer in early 2005. Extended version available on http://eprint.iacr.org/2003/125/* ***5.*** *Frederik Armknecht, Matthias Krause. Algebraic Atacks on Combiners with Memory // Crypto 2003, LNCS 2729, pp. 162-176, Springer.* ***6.*** *Frederik Armknecht. Improving Fast Algebraic Attacks // FSE 2004, LNCS, Springer.* ***7.*** *Philip Hawkes, Gregory Rose. Rewriting Variables: the Complexity of Fast Algebraic Attacks on Stream Ciphers // in Crypto 2004, LNCS 3152, pp. 390-406, Springer, 2004. Available from http://eprint.iacr.org/2004/081/* ***8.*** *Pometun S. Generalized Correlation and Higher Order Nonlinearity for Probabilistic Algebraic Attacks Description // http://eprint.iacr.org/2007/448* ***9.*** *Meier W., Pasalic E., Carlet C. Algebraic Attacks and Decomposition of Boolean Functions // Eurocrypt 2004, LNCS 3027, pp. 474–491, Springer, 2004* ***10.*** *Пометун С. О. Алгебраїчні атаки на потокові шифратори як узагальнення кореляційних атак. Системні дослідження та інформаційні технології 2008, у друку.* ***11.*** *Nicolas T. Courtois. Cryptanalysis of Sfinks // http://eprint.iacr.org/2005/243*

УДК 681.3

КОД УМОВНИХ ЛИШКІВ І ЦІЛІСНІСТЬ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ

Вячеслав Василенко, Олександр Юдін
Національний авіаційний університет

Анотація: **Досліджені можливості застосування в задачах забезпечення цілісності інформаційних об'єктів в телекомунікаційних мережах узагальненого завадостійкого коду умовних лишків та здійснено аналіз його можливостей.**
Summary: **Explored possibilities of application in telecommunication networks in the tasks of providing of integrity of information's holding object of the generalized ant jamming code of conditional tailings. Description of such code is offered and carried out the analysis of his possibilities.**
Ключові слова: **Викривлення, завадостійкий код, комунікаційна мережа, умовні лишки, цілісність.**

I Вступ

Відповідно до термінології нормативних документів Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України [1] під цілісністю інформації розуміється її властивість, яка полягає у тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Іншими словами, під цілісністю інформації розуміється відсутність в ній будь-яких викривлень (модифікацій), які не були санкціоновані її власником, не залежно від причин або джерел виникнення таких викривлень.

Викривлення інформації, тобто порушення її цілісності, можливі на будь-якому етапі її циркуляції у обчислювальних мережах: при зберіганні, передачі або обробці. Причини таких викривлень можуть бути випадковими або навмисними. У свою чергу, випадкові викривлення можуть бути як природними, пов'язаними з дією природних чинників, так і штучними. До числа природних чинників відносяться атмосферні електромагнітні розряди, іскріння контактів в автомобілях, електротранспорті, недостатня надійність електронних елементів і елементів електричних ланцюгів, порушення реєструючого шару магнітних або оптичних носіїв і багато що інше. І випадкові і штучні мають своїм наслідком викривлення

того або іншого числа символів в цифровому представленні інформації, незалежно від використовуваної системи числення або форми представлення інформації і, в цьому значенні, є загрозами функціональним властивостям захищеності інформаційних ресурсів – їх цілісності і доступності. Надалі розглядаються задачі забезпечення цілісності інформаційних об'єктів в умовах природних впливів.

Наслідком природних впливів в каналах телекомунікаційних мереж (ТКМ) є зменшення співвідношення сигнал/шум (сигнал/завада). Це відношення визначає вірність інформації, яка визначається, наприклад, через ймовірність викривлень двійкових символів (біт) Рвикр, а також інтенсивність цих помилок. Тому задача забезпечення цілісності і доступності інформаційних ресурсів є однією з найактуальніших при розробці і експлуатації АС і їх елементів.

Для забезпечення контролю та поновлення цілісності інформаційних об'єктів, включаючи і відновлення зруйнованої інформації, до складу інформації, яка захищається, включають надмірну інформацію – ознаку цілісності або контрольну ознаку (залежно від прийнятої в задачах контролю цілісності або завадостійкого кодування термінології) − своєрідний образ, відображення цієї інформації, процедура формування якого відома, і який з дуже високою вірогідністю відповідає інформації, що захищається.

При цьому між інформацією, що захищається, і ознаками цілісності або контрольними ознаками встановлюється регулярний (функціональний) односторонній зв'язок (процедури розрахунку контрольної ознаки за початковою інформацією, що захищається, відомі, а процедури розрахунку початкової інформації по контрольних ознаках найчастіше не існує). Контроль цілісності (відсутність викривлень) зводиться при цьому до тих або інших процедур перевірки наявності вказаного регулярного (функціонального) одностороннього зв'язку між ознаками цілісності і прийнятої з каналу зв'язку (або зчитаної з запам'ятовуючого (ЗП) пристрою) інформацією.

Механізми забезпечення цілісності істотно залежать від умов їх застосування, а саме від впливу, випадкових (природних) або штучних (зловмисних) викривлень. Характерною особливістю випадкових викривлень є те, що вони, через відсутність навмисності, порушують регулярний (функціональний) односторонній зв'язок між прийнятою (або зчитаною з ЗП) інформацією і ознаками цілісності, сформованими перед передачею (перед записом в ЗП). Тому при виявленні порушення вказаного зв'язку встановлюється факт наявності таких викривлень, а за певних умов, і їх місця і величини (характер). За відсутності порушення цього зв'язку встановлюється факт відсутності викривлень.

Характерною особливістю навмисних викривлень є те, що зловмисник прагне забезпечити, зімітувати наявність регулярного (функціонального) зв'язку між модифікованою їм початковою інформацією, прийнятою (або зчитаною з ЗП), і ознаками цілісності. З цією метою порушник, використовуючи знання процедур формування контрольних ознак, після необхідної для його цілей модифікації початкової інформації перед передачею одержувачу (перед записом в ЗП) забезпечує формування відповідних ознак. При успішному формуванні вказаних ознак, розкрити наявність модифікації неможливо. Для боротьби з цим власнику (або авторизованому користувачу) необхідно використовувати або секретні (невідомі потенційним порушникам) процедури формування контрольних ознак (що дуже складно забезпечити), або вводити в загальновідомі процедури формування контрольних ознак секретні параметри (ключі перетворення). Не знаючи цих секретних параметрів (ключів перетворення), порушник не зуміє забезпечити, зімітувати наявність регулярного (функціонального) зв'язку між модифікованою ним початковою інформацією, прийнятою (або зчитаною із ЗП), і ознаками цілісності.

Однією з причин виникнення викривлень є завади, викликані зовнішніми джерелами і атмосферними явищами. Труднощі боротьби з завадами полягають в безладності, нерегулярності і в структурній схожості завад з інформаційними сигналами. Тому захист інформації від викривлень і шкідливого впливу завад має велике практичне значення і є однією з серйозних проблем сучасної теорії і техніки інформаційного обміну в каналах ТКМ.

Серед основних способів (механізмів) забезпечення цілісності (і в певному значенні − доступності) інформації в умовах природних дій (проблема завадостійкості) для каналів ТКМ (взагалі для мереж передачі даних) слід виділити застосування різного роду завадостійких кодів з виявленням помилок в прийнятій (зчитаній) інформації, які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засоби виявлення викривлень. Це, в свою чергу дає можливість застосування способів передачі повідомлень з різного роду зворотним зв'язком (інформаційного – деякого аналогу мажоритарного методу з багатократною передачею інформації і зворотним прийомом і ухваленням рішення щодо правильності передачі на стороні передавача, або з вирішальним зворотним зв'язком (ВЗЗ) – багаторазовій, при необхідності, передачі з ухваленням рішення щодо правильності передачі на боці приймача). Недоліки таких способів забезпечення цілісності зводяться до необхідності організації другого (зворотного) каналу зв'язку, тобто до істотних матеріальних витрат, а також до збільшення часу затримки передавання інформаційних об'єктів, який може бути неприпустимо великим, а також застосування різного роду завадостійких корегуючих кодів (ЗКК), які

дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засоби виявлення і усунення викривлень.

Останній із способів (механізмів) забезпечення цілісності інформаційних об'єктів − із застосуванням завадостійких корегуючих кодів – наразі знайшов широке застосування в стандартах радіозв'язку, стільникового зв'язку. Він не потребує зворотного каналу і забезпечує, як правило, прийнятне значення часу затримки передавання інформаційних об'єктів. Тому, чи не єдиною проблемою в цих та інших ТКМ з використанням телефонних кабельних та радіоканалів є проблема забезпечення цілісності інформаційних об'єктів в умовах впливу навіть природних (не говорячи уже про штучні, навмисні завади) пакетних викривлень, як "коротких" (тривалістю 2...10 мс) так і особливо "довгих" (тривалістю 100…200 мс). Це є особливо актуальним і для вже згаданих систем стільникового зв'язку. Наприклад, в стандартах CDMA базовий цифровий потік розбивається на пакети тривалістю по 20 мс и подається на згорточний кодер с половинною швидкістю [2]. При цьому тривалість пакету викривлень може бути порівняною чи, навіть, значно перевищувати тривалість інформаційного пакету, що може суттєво вплинути на результативність процедур обміну інформацією.

Як вихід із таких ситуацій може розглядатися можливість збільшення тривалості інформаційних пактів із одночасним застосуванням перемежування потрібної глибини та завадостійких корегуючих кодів, які були б спроможними забезпечити виявлення та виправлення пакетів викривлень значної тривалості. Як такі коди в статті пропонуються узагальнені завадостійкі корегуючі коди.

II Основна частина

Під узагальненими розумітимемо коди, призначені для виявлення (виявлення і виправлення) пакетних викривлень з кратністю b, в яких використовуються алгоритми кодування і декодування, аналогічні відповідним алгоритмам двійкових кодів, але по відношенню до узагальнених b-розрядних символів.

В цих кодах початкова двійкова кодова послідовність − базове кодове слово I1 I2 … Im розбивається на n = m/b узагальнених символів (УС) – груп двійкових розрядів з розрядністю b, в яких передбачається виявлення та виправлення викривлень:

$$\underbrace{I_1 \dots I_b}_{1\text{ – й УС}},\ \underbrace{I_{b+1} \dots I_{2b}}_{2\text{ – й УС}} \dots \underbrace{I_{m-b+1} \dots I_m}_{n\text{ – й УС}}.$$

Двійкові символи, що входять в одну b-розрядну групу, розглядаються як b-значний УС, який може приймати будь-яке із s значень від 0 до (s – 1), де s = 2b.

Одним із прикладів узагальнених кодів є код умовних лишків (код умовних лишків, ЛУ-код). Теоретичною основою ЛУ-коду є теорія лишкових класів. З теорії лишкових класів відомо, що будь-яке число можна представити у вигляді набору лишків від розподілу цього числа на набір взаємно простих чисел, які мають назву основ системи числення, – pi, де i = 1, 2, …, n, n – кількість таких основ. Вибір величини n здійснюється з умови, яка викладена нижче. Тоді

$$A = \alpha_1, \alpha_2, \dots, \alpha_n, \qquad (1)$$

де $\alpha = A - [A/pi]\cdot pi$, а позначка [A/pi] означає операцію розрахунку цілої частини від дробового числа A/pi.

При цьому між числом A і його уявленням (1) існує взаємна однозначна відповідність, якщо

$$A \le P = \prod_{i=1}^{n} p_i .$$

У цьому виразі величина P – діапазон представлення або робочий діапазон чисел. Звернемо увагу на те, що величина αi є собою групою двійкових розрядів, кількість яких не перевищує розрядності відповідної основи pi.

Чудовою властивістю системи лишкових класів (СЛК) є те, що в неї легко вводяться властивості виявлення і виправлення викривлень. Відомо, що якщо ввести ще одну, контрольну, основу pk, то уявлення A в розширеному діапазоні $R = P\cdot pk$, у вигляді

$$A = \alpha_1, \alpha_2, \dots, \alpha_n, \alpha_k, \qquad (2)$$

де αk – лишок по основі pk, має чудову для побудови корегуючих кодів властивість: при pk > pn будь-яке викривлення в одному з лишків αi може бути знайдено, а при $pk > 2\cdot pn\cdot pn\text{-}1$, де pn, pn-1 – найбільші з основ, може бути і виправлено. Це означає, що при представленні чисел у вигляді (2) створюється завадостійкий код з можливостями або виявлення викривлень, або і їх корекції.

Такий код має принаймні 2 недоліки. Перший з них пов'язаний з необхідністю роботи з числами в системі числення в залишкових класах, а другий – з тим, що можливі викривлення знаходяться і

виправляються (викривлений символ поновлюється) тільки в тому випадку, якщо викривлений лише один з символів αi, тобто викривлення повинні бути фіксованими в межах однієї з груп розрядів.

Цей недолік достатньо просто усувається в коді умовних лишків, який вводиться таким чином.

Хай є код деякого числа А, представленого в будь-якій системі числення, зокрема позиційної, наприклад двійкової. Для визначеності, хай це число А представлено послідовністю з нулів і одиниць. Розіб'ємо цю послідовність певним, у загальному випадку довільним, чином на n груп, як і для решти узагальнених кодів.

Як і раніше код кожної і – ї групи (пакету) розглядатимемо як s – значний розряд αi, який може приймати будь-яке з s значень від 0 до s – 1, де s = 2b, але умовно вважатимемо цей код лишком деякого умовного числа А по основі pi. Оскільки величина αi, як елемент початкового числа

$$0 \le \alpha_i \le s - 1,$$

а як лишок від ділення А на pi

$$0 \le \alpha_i \le p_i,$$

то для представлення коду будь-якої групи у вигляді лишку по основі p_i необхідно, щоб виконувалася умова

$$p_i > s - 1,$$

інакше в групу із b розрядів може бути записаним код $\alpha_i \ge p_i$, що в лишкових класах не допустимо.

Приклад. Хай b =3, s = 7, тоді αi може приймати значення 000, 001, 010,..., 11. При pi = 5 максимальне значення αi обмежується кодом 100, тобто коди 101, 110, 111 є "неправильними". Якщо ж взяти pi > 7, наприклад pi = 9, тоді максимальне значення αi обмежується не величиною pi, а розрядністю групи b, тобто αmax = 11.

При такому підході будь-які комбінації початкового коду числа А "вписуються" в систему числення з основами pi (i = 1, 2,...). Якщо розширити систему основ на контрольну pk і для одержаного набору умовних лишків αi (i = 1, 2,...) розрахувати умовний лишок αk, то на одержане умовне число

$$A = \alpha_1, \alpha_2, \ldots, \alpha_{n1}, \alpha_к \qquad (3)$$

розповсюджується можливість СЛК з виявлення і виправленню викривлення, тобто одержаний код (3) має всі властивості коду (2), але останній код може бути отриманий для будь-якої двійкової послідовності, а не тільки по відношенню до чисел в лишкових класах. Відзначимо, що таким чином усунено перший недолік коду (2).

Оскільки для отримання контрольної ознаки, тобто для кодування будь-якої послідовності двійкових цифр завадостійким кодом, умовно, не реально, не фізично групи розрядів початкового числа розглядаються як деякі лишки, то такий код одержав найменування коду умовних лишків.

Слід звернути увагу на те, що при кодуванні ЛУ-кодом початкова послідовність не змінюється, до неї тільки приформовуються додаткові, обчислені за окремими правилами, контрольні символи.

Таким чином ЛУ-код дозволяє знаходити і виправляти b-розрядні пакети викривлень, згруповані в межах будь-якої з n груп і вимагає при цьому надмірність біля

$$r \approx 2b + 1$$

розрядів (оскільки $p_k \approx 2 p_n p_{n-1}$, $r = [\log_2 p_k] + 1$). В конкретних випадках ця надмірність може відхилятися в ту або іншу сторону, що залежить також від алгоритмів кодування-декодування.

Оскільки в основі ЛУ-коду лежать властивості СЛК, то в цьому коді принципово можуть бути використані відомі алгоритми кодування-декодування. В основі цих алгоритмів лежить той факт, що будь-яке викривлення в одній з груп розрядів αi переводить початкове число з робочого діапазону $[0, P = \prod_{i=1}^{n} p_i)$ в діапазон [P, R), де R = pk·P, тобто приводить до збільшеня початкового числа A < P на деяку величину li·Ri. Тут li і Ri = R/pi – цілі числа. Дійсно, якщо вихідне число

$$A = \alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_k$$

є викривленим по основі pi і має вид

$$\tilde{A} = \alpha_1, \alpha_2, \ldots, \tilde{\alpha}_i, \ldots, \alpha_n, \alpha_к$$

де

$$\tilde{\alpha}_i = \{\alpha_i + \Delta\alpha_i\} \pmod{p_i},$$

то це є еквівалентним наступному перетворенню

$$\tilde{A} = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_k) + + (0, 0, \ldots, \Delta\alpha_i, \ldots, 0, 0) =$$
$$= (\alpha_1, \alpha_2, \ldots, \{\alpha_i + \Delta\alpha_i\} \pmod{p_i}, \ldots, \alpha_{n1}, \alpha_k).$$

При цьому величина викривлення перевищує величину робочого діапазону P:

$$\Delta A = (0, 0, \ldots, \Delta\alpha_i, \ldots, 0, 0) > P,$$

оскільки тільки число виду

$$\Delta A = l_i \cdot R_i = l_i \cdot R/p_i$$

має всі лишки, окрім лишка по основі pi такими, що дорівнюють нулю. Але ΔA = li·Ri > P = R/pk тобто, навіть при li = 1, величина R/pi > R/pk по тій причині, що pk > pi.

Відтак, сума $\tilde{A}$ = A + ΔA > P, тобто викривлене число вийшло за межі робочого діапазону P і попало в діапазон [P, R).

Відомі алгоритми кодування-декодування як раз і використовують цей факт.

III Висновки

Застосування запропонованих узагальнених кодів дозволяє забезпечити виявлення та виправлення викривлень в b-розрядних узагальнених символах в кожному із базових кодових слів.

Застосування таких кодів, на погляд авторів, дозволить розв'язати проблему надійного забезпечення цілісності інформаційних об'єктів в умовах впливу пакетів викривлень значної тривалості.

Література: ***1****. НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".* ***2****. Дубровский В. В. CDMA − взгляд глазами профессионала. //mailto:v_ dubrovskii@mail.ru.*

УДК 681.3.06

АНАЛИЗ ОДНОГО МЕТОДА ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ОСНОВАННОГО НА КОНТЕКСТНОМ МОДЕЛИРОВАНИИ

Михаил Савчук, Виталий Шарапов

Физико-технический институт Национального технического университета Украины "КПИ"

Анотація: **Розробляється статистичний критерій тестування двійкових послідовностей на випадковість, що базується на правильності завбачення знаків за попередніми бітами. Знаходяться теоретичні та експериментальні розподіли статистик.**

Summary: **In the work the statistical criterion of testing binary sequences on the randomness, based on correctness prediction signs on the previous bits are offered. There are theoretical and experimental statistic distributions.**

Ключевые слова: **Контекстное моделирование, контекстное сжатие, случайные и псевдослучайные последовательности, тестирование случайных последовательностей, статистический критерий.**

I Постановка задачи. Основные определения

В настоящее время разработан ряд статистических тестов для проверки качества случайных и псевдослучайных последовательностей, например, пакет NIST Statistical Test Suite [1]. Однако задача построения новых критериев для оценивания характеристик таких последовательностей остается актуальной для многих применений и исследований, особенно, в области криптографической защиты информации. Новые и модифицированные критерии могут лучше "работать" при других параметрах последовательностей (например, малой длине) или лучше отличить определенные виды альтернативных гипотез. В [2] предложен метод тестирования последовательностей, основанный на контекстном моделировании [3]. В данной работе разрабатываются другие критерии, в основе которых лежит идея контекстного сжатия, проведен теоретический анализ, приведены алгоритмы для построения статистик и критических областей.

Пусть задана последовательность $\varepsilon = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_n$, $\varepsilon_i \in \{0,1\}$, $i = 1, \ldots, n$, которую рассматриваем как реализацию некоторого случайного дискретного процесса. Необходимо проверить гипотезу H0 о том, что последовательность ε является реализацией последовательности независимых равновероятных двоичных знаков, т. е. случайные величины ε_i независимы в совокупности и $\forall i = 1, \ldots, n \; P(\varepsilon_i = 0) = P(\varepsilon_i = 0) = 1/2$.

Назовем контекстом $k_m(i)$ порядка m, $0 \le m < n$, символа ε_i, $i = m+1, \ldots, n,$ число, двоичная запись