виділення фрагментів схем. Побудовано максимально детальні векторизовані технологічні схеми всіх підрозділів ДК "Укртрансгаз". Розроблено і програмно реалізовано модель автоматизації робочого місця диспетчера (АРМу), а також базу даних підтримки схем ГТС України. Розроблено і програмно реалізовано механізм обміну інформацією між підрозділами управління ГТС України.

Для ефективного використання бази технологічних схем потрібно виконано додаткові роботи: забезпечити підтримку технологічних схем в актуальному стані; забезпечити інформаційну підтримку режимних і прогнозних задач, які розв'язуються у підрозділах ДК "Укртрансгаз".

1. Панкратов В.С., Герке В.Г., Митичкин С.К., Сарданашвили С.А. Комплекс моделирования и оптимизации режимов работы ГТС. – М.: Газпром, 2002. – 56 с. – (Газовая промышленность. Сер. Автоматизация, телемеханизация и связь в газовой промышленности Изд-во ООО ИРЦ). 2. Панкратов В.С., Берман Р.Я. Разработка и эксплуатация АСУ газотранспортными системами, – Л.: Недра, 1982. – 142 с. 3. Притула Н.М. Розрахунок параметрів потокорозподілу в газотранспортній системі (стаціонарний випадок)// Фізико-математичне моделювання та інформаційні технології. – Львів, 2007. – Вип. 5. – С. 146–157. 4. Притула Н. М., Притула М. Г., П'янило Я.Д. Розрахунок параметрів усталеного руху газу в магістральних газопроводах // Вісн. Нац. ун-ту "Львівська політехніка". – Львів, 2006. – № 565: Комп'ютерні науки та інформаційні технології. – С. 270–274.

УДК 519.15:621.372

О.Я. Різник, Д.С. Балицька
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

СИНТЕЗ БАГАТОПОЗИЦІЙНИХ БАГАТОКРАТНИХ КОДІВ НА ОСНОВІ ЧИСЛОВИХ В'ЯЗАНОК

Розглянуто перетворення інформації на основі багатопозиційних багатократних кодів для кодування інформації. Розроблена методика побудови кодових комбінацій чисел на основі теорії числових в'язанок, що уможливлює подання кодових комбінацій чисел у вигляді багатопозиційного багатократного коду.

Ключові слова: в'язанка, кодування, лінійка Голомба, багатопозиційний багатократний код.

In the article transformations of information are examined on the basis of noise codes for realization of code of information. The worked out methods of construction of code combinations of numbers are on the basis of theory of numerical bundles, which enables presentation of code combinations of numbers as a noise code.

Keywords: bundle, code, Golomb ruler, noise code.

Вступ

Сьогодні криптографія необхідна приватному комерційному сектору економіки України для прогресивного розвитку. Це стосується використання криптографічних алгоритмів, їхніх прикладних вживань, загальних методів управління ключами і їх розподілу. Секретні ключі є основою криптографічних перетворень, для яких, згідно з правилом Керкхофа, стійкість хорошої шифрувальної системи визначається лише секретністю ключа. Основна проблема класичної криптографії довгий час полягала в складності генерування непередбачуваних двійкових послідовностей великої довжини із застосуванням короткого випадкового ключа. Для її вирішення широко застосовують

генератори двійкових псевдовипадкових послідовностей. Тому в цій статті розглянуто правила побудови довгих псевдовипадкових послідовностей, використовуваних криптографічними системами для перетворення повідомлень.

Криптографічні перетворення спрямовані на досягнення двох цілей із захисту інформації. По-перше, вони забезпечують недоступність її для осіб, що не мають ключа і, по-друге, підтримують з необхідною надійністю виявлення несанкціонованих спотворень. Порівняно з іншими методами захисту інформації класична криптографія гарантує захист лише за умов, що:

- використаний ефективний криптографічний алгоритм;
- дотримані секретність і цілісність ключа.

Некриптографічні засоби не дають такої самої міри захисту інформації і вимагають значно більших витрат. Науково-технічною основою появи сучасних мереж передавання інформації є забезпечення максимальної пропускної спроможності систем передачі C за наявної смуги пропускання лінії зв'язку ΔF відповідно до формули Найквіста, одержаної з використанням теореми В.О. Котельнікова:

$$C = 2\Delta F \log M \quad [\text{біт/с}], \tag{1}$$

де M – кількість дискретних значень коду.

Ця формула справедлива за умов відсутності завад у лінії зв'язку. За наявності завад максимальна пропускна спроможність системи передачі визначатиметься формулою Шеннона:

$$C = \Delta F \log\left(1 + \frac{P_с}{P_ш}\right) \quad [\text{біт/с}], \tag{2}$$

де $P_с$, $P_ш$ – середня потужність коду та завад.

Важливою вимогою для систем шифрування та кодування є забезпечення їхньої максимальної завадостійкості. Для підвищення завадостійкості систем передачі використовують завадостійке кодування, за якого до інформаційного повідомлення додають зайві перевірні біти для виправлення помилок, що, однак, призводить до розширення спектра сигналу. Найпоширеніші блокові коди БЧХ (Боуза–Чоудхурі–Хоквенгема), коди Ріда–Соломона, а також безперервні згорткові коди з декодуванням їх за алгоритмом Вітербі.

Постановка проблеми

Особливо цікавим є об'єднання методів кодування і шифрування. Можна стверджувати, що, по суті, кодування – це елементарне шифрування, а шифрування – це елементарне завадостійке кодування. Розроблення і реалізація таких універсальних методів – перспектива сучасних інформаційних систем.

Особливість багатопозиційних багатократних кодів полягає в тому, що вони поєднують завадостійке кодування та шифрування. Упевнене виявлення таких кодів можливе у разі введення надмірності, тобто за використання для передачі повідомлень послідовності істотно надлишкової, ніж передане повідомлення.

Перевагою багатопозиційного багатократного коду є можливість застосовувати новий вигляд селекції – за допомогою послідовності. Цікавою особливістю цих кодів є їхні адаптивні властивості – із зменшенням кількості завад завадостійкість зростає.

Недоліком є перехід до складнішого носія інформації, що призводить, природно, до відомого ускладнення систем передачі повідомлень.

Розв'язання поставленої задачі

Цим вимогам більшою мірою відповідають багатопозиційні багатократні коди, побудовані на основі числових в'язанок. В загальному випадку простою ідеальною числовою в'язанкою (ЧВ) порядку N кратності R на послідовності N чисел називається така послідовність $K_N = (k_1, k_2, ..., k_i, ..., k_N)$, на якій суми набувають R різних значень всіх L_N чисел, починаючи із заданого числа. У простішому варіанті ці суми вичерпують R разів значення чисел натурального ряду $1, 2, ..., L_N$ [1].

Метод побудови багатопозиційних багатократних кодів на основі числових в'язанок за критерієм мінімального значення функції автокореляції дискретного коду полягає у такому: побудувати L_N-позиційний код m_i, $i = 1, 2, ..., L_N$ на основі вибраного варіанта ЧВ $(k_1, k_2, ..., k_l, ..., k_N)$, де на N позиціях коду з порядковими номерами x_l, $l = 1,2,...,N$, які визначаються з формули

$$x_l \equiv 1 + \sum_{i=1}^{l} k_i \pmod{L_N}, \tag{3}$$

розмістити символи "1", а на решті $L_N - N$ позиціях – символи "0" [2, 3].

Одержана послідовність є багатопозиційною багатократною кодовою послідовністю з властивістю “не більше ніж R -збігів”. Вибираючи різні варіанти числових в'язанок з такими параметрами, можемо одержати інші кодові послідовності з властивістю “не більше ніж R - збігів” [3].

Властивості цих багатопозиційних багатократних кодових послідовностей:

- у послідовності кількість чисел 1 і 0 відрізняється не більш ніж на одиницю;
- серед груп з послідовних 1 і 0 в кожному періоді половина має тривалість в один символ, четверта частина має тривалість в два символи, восьма частина має тривалість в чотири символи і так далі;
- кореляційна функція послідовності має єдиний значний пік амплітуди 1 і при всіх зрушеннях дорівнює $1/m$, де m – довжина послідовності);
- кореляція між зсунутими циклічно кодовими послідовностями обчислюється за формулою:

$$r(c, y) = \frac{A - B}{A + B}, \tag{4}$$

де A – кількість позицій, в яких символи послідовностей x і y збігаються; B – кількість позицій, в яких символи послідовностей x і y різні.

Ми використаємо відомі багатократні числові в’язанки для генерації багатопозиційних багатократних кодів, оскільки числові в’язанки за визначенням повинні мати всі різні відліки “не більше ніж R - збігів” [3].

Запропонований метод побудови багатопозиційних багатократних кодів оснований на перетворенні числових в’язанок. Для побудови багатопозиційних багатократних кодів за допомогою числових в’язанок порядку N кратності R виділимо рядок із L_N пронумерованих за зростанням порядку клітинок одновимірного масиву і заповнимо інформаційними "одиницями" клітинки, номери яких збігаються з числами, визначеними з числової в’язанки. У клітинки, що залишилися незаповненими, внесемо "нулі". Утворена послідовність одиниць і нулів є L_N-розрядним багатопозиційним багатократним кодом, циклічним зсувом якого можна одержати й решту дозволених комбінацій.

Прикладом такого коду є таблиця кодових комбінацій, складена за допомогою лінійки Голомба порядку $N = 6$ кратності $R = 3$ (1, 1, 2, 2, 1, 3) (табл. 2).

Таблиця 2

Багатопозиційні багатократні коди
на основі числової в’язанки з $N = 6$ та $R = 3$

1	1	1	0	1	0	1	1	0	0
0	1	1	1	0	1	0	1	1	0
0	0	1	1	1	0	1	0	1	1
1	0	0	1	1	1	0	1	0	1
1	1	0	0	1	1	1	0	1	0
0	1	1	0	0	1	1	1	0	1
1	0	1	1	0	0	1	1	1	0
0	1	0	1	1	0	0	1	1	1
1	0	1	0	1	1	0	0	1	1
1	1	0	1	0	1	1	0	0	1

Будь-яка з L_N різних кодових комбінацій багатопозиційного багатократного коду містить точно N одиничних символів в однойменних розрядах, що випливає з властивостей числової в'язанки. Решта $L_N - N$ кодових комбінацій багатопозиційного багатократного коду містять нулі [2].

Мінімальна кодова відстань для цього багатопозиційного багатократного коду визначається як:

$$d_{\min} = 2(N\text{-}2) = 2(6-3) = 6. \quad (5)$$

Кількість помилок, які можна виявити t_1, і кількість помилок, що можна виправити t_2 за допомогою багатопозиційного багатократного коду, визначається мінімальною кодовою відстанню:

$$t_1 \le d_{\min} - 1 = 6 - 1 = 5, \quad (6)$$

$$t_2 \le (t_1 - 1)/2 = (5-1)/2 = 2. \quad (7)$$

Розроблений програмний продукт для кодування та декодування з виправленням помилок за допомогою багатопозиційних багатократних кодів, де необхідно задати:

- вхідні дані (елементи числової в'язанки);
- кількість помилок, які знаходять та виправляють;
- шлях до файла, який необхідно закодувати та декодувати на основі багатопозиційного багатократного коду.

Висновки

Багатопозиційні багатократні коди належать до безлічі з украй нерегулярною розгалуженою структурою. Основні поняття теорії поки що у процесі становлення та розвитку, але поле їхнього застосування безперервно розширюється. Великий інтерес до цих кодів пов'язаний з тим, що їхні аналоги, такі як квазікоди Баркера, лінійки Голомба, числові в'язанки використовуються у реальних завданнях, причому в типових, а не в екзотичних ситуаціях.

Дослідження різних типів багатопозиційних багатократних кодів свідчить про переваги тих із них, які синтезовані на основі числових в'язанок, що дає змогу досягти більшої криптостійкості та завадостійкості під час перетворення інформації порівняно з класичними кодовими послідовностями.

1. Різник В.В. Синтез оптимальних комбінаторних систем. – Львів, 1989. 2. Різник В.В., Різник О.Я., Кісь Я.П., Дурняк Б.В., Парубчак В.О.. Використання монолітних кодів в інформаційних технологіях. МНТК ISDMIT'2006. – Євпаторія, 2006. – Т. 2. – С. 39–42. 3. Різник О.Я., Балич Б.І. Використання числових лінійок-в'язанок для кодування інформації // Вісн Нац. ун-ту "Львівська політехніка". – 2006. – Комп'ютерні науки та інформаційні технології. – С. 62–64.