УДК 621.391

В.М. Рудницький, В.Г. Бабенко

Черкаський державний технологічний університет, Черкаси

СИНТЕЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ ПРИСТРОЇВ ДЕКОДУВАННЯ ІНФОРМАЦІЇ ДЛЯ КРИПТОГРАФІЧНИХ СИСТЕМ

Робота присвячена розробці теоретичних основ побудови пристроїв декодування на основі синтезованих моделей логічних функцій спеціального класу для систем захисту інформації. Результати дослідження та математичного моделювання експериментальних даних дозволили визначити і довести загальні закономірності побудови функцій декодування на основі використаних функцій кодування.

Ключові слова: *інформаційна безпека, криптографія, спеціалізовані логічні функції.*

Вступ

Постановка проблеми. Впровадження і активне використання сучасних інформаційних технологій істотно підвищили уразливість інформації, циркулюючої в сучасних інформаційно-телекомунікаційних системах.

Несанкціоноване спотворення, копіювання, знищення інформації в даний час зачіпає не тільки процеси, що відносяться до сфери державного управління, але і інтереси фізичних осіб. Як наслідок, зростає відповідальність за ухвалення точних і відповідальних рішень в ситуаціях, коли навіть окремі помилки здатні привести до тяжких наслідків у сфері економіки, фінансів, екології.

Підключення до відкритих (глобальних) мереж, таких як Інтернет, істотно збільшує ефективність роботи і відкриває безліч нових можливостей. В той же час необхідно поклопотатися про створення системи захисту інформаційних ресурсів від охочих їх використовувати, модифікувати або просто знищити. Захист інформації несе в собі підтримку цілісності, доступності і, якщо необхідно, конфіденційності інформації і ресурсів, що використовуються для введення, зберігання, обробки і передачі даних. Для вирішення комплексної проблеми захисту необхідне поєднання законодавчих, організаційних і програмно-технічних заходів.

У сучасних умовах захист інформації стає все більш актуальною і одночасно все більш складною проблемою. Це зумовлено як масовим застосуванням методів автоматизованої обробки даних так і широким розповсюдженням методів і засобів несанкціонованого доступу до інформації. Тому останнім часом все більше уваги приділяють забезпеченню безпеки комунікацій, зберігання даних, конфіденційності доступу до даних і подібних аспектів. Пропонуються численні рішення, як на апаратному рівні, так і на рівні програмного забезпечення [1].

Аналіз досліджень та публікацій. Побудова сучасної криптології як науки засноване на сукупності фундаментальних понять і фактів математики, фізики, теорії інформації, складності обчислень та теорії кодування, природно дуже складних для всестороннього та глибокого осмислення навіть професіоналами. Однак, не дивлячись на органічно притаманну їй складність, безліч теоретичних досліджень криптології зараз широко використовуються в нашому насиченому інформаційними технологіями житті, наприклад: в пластикових smart-картах, в електронній пошті, в системах електронного документообігу, при введенні баз даних, системах електронного голосування та інше. Тому у відкритому суспільстві одним із необхідних, навіть визначних умов використання інформаційних технологій в соціальних системах та бізнесі, як і в інших галузях, є дотримання умов та використання засобів забезпечення інформаційної безпеки [2].

Без криптографії принципово неможливо обійтись при захисті даних, які передаються по відкритим каналам зв'язку, а також там, де необхідно підтверджувати цілісність електронної інформації або доводити її авторство [3].

Мета роботи полягає у розробці математичного апарату побудови пристроїв криптографічного декодування інформації, кодування якої виконано на основі наборів спеціалізованих логічних функцій.

Виклад основного матеріалу

Для доведення коректності математичних моделей функцій декодування було використано векторне представлення функцій кодування – декодування [4]

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus b_2 \end{pmatrix}. \qquad (1)$$

В попередніх роботах [5 – 7] були доведені нижче зазначені леми, що підтверджують правильність математичних моделей пристроїв декодування та коректність використання зазначених пристроїв кодування-декодування в системах криптографічного захисту.

Лема 1. Якщо $\vec{F}_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, то перетворення при кодуванні і декодуванні співпадають.

Лема 2. Якщо функція кодування представлена $\vec{F}_2\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\\x_1\end{pmatrix}$, то вона співпадає з функцією декодування .

Лема 3. Якщо функція кодування представлена $\vec{F}_3\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus 1\\x_2\end{pmatrix}$, то вона співпадає з функцією декодування.

Лема 4. Якщо функція кодування представлена $\vec{F}_4\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\\x_2\oplus 1\end{pmatrix}$, то вона співпадає з функцією декодування.

Лема 5. Якщо функція кодування представлена $\vec{F}_5\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus 1\\x_2\oplus 1\end{pmatrix}$, то вона співпадає з функцією декодування.

Лема 6. Якщо функція кодування представлена $\vec{F}_6\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\oplus 1\\x_1\oplus 1\end{pmatrix}$, то вона співпадає з функцією декодування.

Лема 7. Якщо функція кодування представлена $\vec{F}_{7.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\\x_1\oplus 1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{7.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\oplus 1\\x_1\end{pmatrix}$.

Лема 8. Якщо функція кодування представлена $\vec{F}_{8.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\oplus 1\\x_1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{8.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\\x_1\oplus 1\end{pmatrix}$.

Лема 9. Якщо функція кодування представлена $\vec{F}_9\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\x_2\end{pmatrix}$, то вона співпадає з функцією декодування.

Лема 10. Якщо функція кодування представлена $\vec{F}_{10.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\\x_1\oplus x_2\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{10.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\x_1\end{pmatrix}$.

Лема 11. Якщо функція кодування представлена $\vec{F}_{11.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{11.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\x_2\oplus 1\end{pmatrix}$.

Лема 12. Якщо функція кодування представлена $\vec{F}_{12.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{12.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\x_1\oplus 1\end{pmatrix}$.

Лема 13. Якщо функція кодування представлена $\vec{F}_{13.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\x_2\oplus 1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{13.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{pmatrix}$.

Лема 14. Якщо функція кодування представлена $\vec{F}_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_2\end{pmatrix}$, то вона співпадає з функцією декодування.

Лема 15. Якщо функція кодування представлена $\vec{F}_{15.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\\x_1\oplus x_2\oplus 1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{15.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_1\end{pmatrix}$.

Лема 16. Якщо функція кодування представлена $\vec{F}_{16.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\oplus 1\\x_1\oplus x_2\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{16.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{pmatrix}$.

Лема 17. Якщо функція кодування представлена $\vec{F}_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\\x_1\oplus x_2\end{pmatrix}$, то вона співпадає з функцією декодування.

Лема 18. Якщо функція кодування представлена $\vec{F}_{18.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\x_1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{18.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\\x_1\oplus x_2\end{pmatrix}$.

Лема 19. Якщо функція кодування представлена $\vec{F}_{19.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{19.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus 1\\x_1\oplus x_2\end{pmatrix}$.

Лема 20. Якщо функція кодування представлена $\vec{F}_{20.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{20.2}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_2\oplus 1\\x_1\oplus x_2\end{pmatrix}$.

Лема 21. Якщо функція кодування представлена $\vec{F}_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\\x_1\oplus x_2\oplus 1\end{pmatrix}$, то вона співпадає з функцією декодування.

Лема 22. Якщо функція кодування представле-

на $\vec{F}_{22.1}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{22.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$.

Лема 23. Якщо функція кодування представлена $\vec{F}_{23.1}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{23.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$.

Лема 24. Якщо функція кодування представлена $\vec{F}_{24.1}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{pmatrix}$, то функція декодування буде представлена $\vec{F}_{24.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$.

Спираючись на розроблені математичні моделі пристроїв кодування з використанням спеціалізованих логічних функцій для систем криптографічного захисту потрібно розробити методику побудови пристроїв декодування. Для цього введемо наступні визначення.

Визначення 1. Правильно розміщеною функцією називається функція, номер якої співпадає з номером одного із аргументів.

Визначення 2. Неправильно розміщеною функцією називається функція, номер якої не співпадає з номером аргументів.

Визначення 3. Функція називається простою, якщо вона залежить лише від одного аргументу.

Визначення 4. Функція називається складною, якщо вона залежить лише від декількох аргументів складених по модулю.

Сформулюємо основні залежності взаємозв'язку функцій кодування і декодування, які виявлені на основі аналізу результатів попередніх досліджень.

Лема 25 При кодуванні проста правильно розміщена функція не змінює функції декодування.

Доведення: відповідно до векторного представлення функцій кодування – декодування (1), умови леми будуть виконуватися, якщо $a_{12} = a_{21} = 0$ або $a_{12} = 0$, або $a_{21} = 0$. Справедливість першого випадку, коли $a_{12} = a_{21} = 0$ при умові $b_1 = b_2 = 0$ доведена лемою 1, при $b_1 = b_2 = 1$ доведена лемою 5, при $b_1 \neq b_2$ доведена лемами 3 і 4. Справедливість другого випадку, коли $a_{12} = 0$ при умові $b_1 = b_2 = 0$ доведена лемою 17, при $b_1 = b_2 = 1$ доведена лемою 19, при $b_1 \neq b_2$ доведена лемами 21 і 22. Справедливість останнього випадку, коли $a_{21} = 0$ при умові $b_1 = b_2 = 0$ доведена лемою 9, при $b_1 = b_2 = 1$ доведена лемою 11, при $b_1 \neq b_2$ доведена лемами 13 і 14. Лема доведена.

Наслідок леми 25. При кодуванні інверсія простої правильно розміщеної функції не змінює функції декодування.

Теорема 1. Якщо при кодуванні проста неправильно розміщена функція інвертована, то для декодування необхідно інвертувати функції.

Доведення: Так як дана теорема стосується лише одної з двох функцій, то для її доведення розглянемо всі випадки, коли інша функція не змінює функції декодування.

Можливий один із двох випадків: інвертована перша неправильно розміщена функція, тобто $a_{11} = a_{22} = 0$, $b_1 = 1$ і $b_2 = 0$. Відповідно до теореми буде:

$$\vec{F}_{8.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{8.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus 1\right) = \begin{pmatrix} x_2 \oplus 1 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 8. Для другого випадку інвертована друга неправильно розміщена функція, тобто $a_{11} = a_{22} = 0$, $b_1 = 0$ і $b_2 = 1$. Відповідно до теореми буде:

$$\vec{F}_{7.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{7.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus 1\right) = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 7. Теорема доведена.

Наслідок 1 теореми 1. Якщо при кодуванні дві прості неправильно розміщені функції інвертовані, то функція кодування співпадає з функцією декодування.

Доведення: Так як згідно умови $a_{11} = a_{22} = 0$, і $b_1 = b_2 = 1$,тоді

$$\vec{F}_{6.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{6.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus 1 \oplus 1\right) = \begin{pmatrix} x_2 \oplus 1 \oplus 1 \oplus 1 \\ x_1 \oplus 1 \oplus 1 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}.$$

Наслідок доведено.

Наслідок 2 теореми 1. При кодуванні проста неправильно розміщена функція не змінює функції декодування.

Теорема 2. При кодуванні правильно розміщена складна функція не змінює функцію декодування.

Доведення: Можливий один із чотирьох випадків: складною є перша правильно розміщена функція, тобто $a_{11} = a_{12} = a_{22} = 1$ і $a_{21} = 0$, при умові, що $b_1 = b_2 = 0$. Справедливість даного випадку доведено лемою 9. Випадок, коли складною є друга правильно розміщена функція, тобто $a_{11} = a_{21} = a_{22} = 1$ і $a_{12} = 0$, при умові, що $b_1 = b_2 = 0$ підтверджується лемою 17. Розглянемо випадки, коли інвертована складна функція. Якщо $a_{11} = a_{12} = a_{22} = 1$ і $a_{21} = 0$, при умові, що $b_1 = 1$, $b_2 = 0$, то відповідно до леми 14 функції кодування і декодування співпадають. Для випадку, коли

$a_{11} = a_{21} = a_{22} = 1$ і $a_{12} = 0$, при умові, що $b_1 = 0$, $b_2 = 1$, то відповідно до леми 21 функція декодування відповідає функції кодування.

Наслідок теореми 2. При кодуванні інверсія правильно розміщеної складної функції не змінює функцію декодування.

Теорема 3. Якщо при кодуванні використовувалась неправильно розміщена складна функція, то для декодування необхідно до кожної з функцій кодування додати відповідні прості правильно розміщені функції.

Доведення: Можливі два випадки: складною є перша або друга неправильно розміщена функція. Для першого випадку справедливо

$$a_{11} = a_{12} = a_{21} = 1 \text{ і } a_{22} = b_1 = b_2 = 0.$$

Відповідно до теореми буде:

$$\vec{F}_{18.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{18.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 \oplus x_2 \oplus x_1 \\ x_1 \oplus x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 18.

Для другого випадку справедливо

$$a_{12} = a_{21} = a_{22} = 1 \text{ і } a_{11} = b_1 = b_2 = 0.$$

Відповідно до теореми буде:

$$\vec{F}_{10.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{10.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_2 \oplus x_1 \\ x_1 \oplus x_2 \oplus x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 10.

Теорема 4. Якщо при кодуванні правильно розміщена функція інвертована, а інша являється складною, то для декодування необхідно додатково інвертувати складну функцію.

Доведення: Розглянемо два випадки: складною є перша або друга функція. Для першого випадку справедливо $a_{11} = a_{12} = a_{22} = b_2 = 1$ і $a_{21} = b_1 = 0$.

Відповідно до теореми запишемо:

$$\vec{F}_{13.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{13.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \oplus 0 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 13.

Для другого випадку дійсно

$$a_{11} = a_{21} = a_{22} = b_1 = 1 \text{ і } a_{12} = b_2 = 0.$$

Відповідно до теореми запишемо:

$$\vec{F}_{22.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{22.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} x_1 \oplus 1 \oplus 0 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 22.

Розглянемо випадки, коли

$$a_{11} = a_{12} = a_{22} = b_1 = b_2 = 1 \text{ і } a_{21} = 0$$

або $a_{11} = a_{21} = a_{22} = b_1 = b_2 = 1$ і $a_{12} = 0$.

Для третього випадку справедливий запис:

$$\vec{F}_{11.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{11.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \oplus 1 \\ x_2 \oplus 1 \oplus 0 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 11.

Для останнього випадку можемо записати:

$$\vec{F}_{19.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{19.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} x_1 \oplus 1 \oplus 0 \\ x_1 \oplus x_2 \oplus 1 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 19.

Теорема 5. Якщо при кодуванні неправильно розміщена функція інвертована, а інша являється складною, то для декодування необхідно інвертувати складну функцію та до кожної з функцій кодування додати відповідні правильно розміщені функції.

Доведення: Розглянемо два випадки: складною є перша або друга функція. Для першого випадку справедливо $a_{11} = a_{12} = a_{22} = b_2 = 1$ і $a_{21} = b_1 = 0$.

Відповідно до теореми запишемо:

$$\vec{F}_{23.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{13.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \oplus x_1 \\ x_1 \oplus 1 \oplus x_2 \end{pmatrix} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 23.

Для другого випадку дійсно

$$a_{11} = a_{21} = a_{22} = b_1 = 1 \text{ і } a_{12} = b_2 = 0.$$

Відповідно до теореми запишемо:

$$\vec{F}_{16.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{22.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_2 \oplus 1 \oplus x_1 \\ x_1 \oplus x_2 \oplus 1 \oplus x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 16.

Розглянемо випадки, коли

$$a_{11} = a_{12} = a_{21} = b_1 = b_2 = 1 \text{ і } a_{22} = 0$$

або $a_{12} = a_{21} = a_{22} = b_1 = b_2 = 1$ і $a_{11} = 0$.

Для третього випадку справедливий запис:

$$\vec{F}_{20.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{11.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \oplus 1 \\ x_2 \oplus 1 \oplus 0 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 20.

Для останнього випадку можемо записати:

$$\vec{F}_{12.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{19.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) =$$

$$= \begin{pmatrix} x_1 \oplus 1 \oplus 0 \\ x_1 \oplus x_2 \oplus 1 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 12.

Теорема 6. Якщо при кодуванні використовувалась інверсія складної неправильно розміщеної функції, то для декодування необхідно до кожної з функцій кодування додати відповідні інвертовані правильно розміщені функції.

Доведення: Розглянемо два випадки: інвертованою складною неправильно розміщеною є перша або друга функція. Для першого випадку справедливо $a_{11} = a_{12} = a_{21} = b_1 = 1$ і $a_{22} = b_2 = 0$.

Відповідно до теореми запишемо:

$$\vec{F}_{24.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{13.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}\right) =$$

$$= \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \oplus x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 4.

Для другого випадку дійсно

$$a_{12} = a_{21} = a_{22} = b_2 = 1 \text{ і } a_{11} = b_1 = 0.$$

Відповідно до теореми запишемо:

$$\vec{F}_{15.2}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \vec{F}_{13.1}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}\right) =$$

$$= \begin{pmatrix} x_2 \oplus x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \oplus x_2 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

Отриманий результат, відповідає вимозі леми 15.

Висновки

Результати дослідження та математичного моделювання експериментальних даних дозволили визначити і довести загальні закономірності побудови функцій декодування на основі використаних функцій кодування.

Сукупність доведених теорем представляє собою методику побудови математичних моделей пристроїв декодування інформації.

Отримані математичні моделі пристроїв кодування і декодування інформації можуть знайти практичне застосування для побудови дискретних пристроїв криптографічних системах захисту інформації. Сумісно з раніше відомими аналогічними функціями вони дозволять в перспективі значно підвищити якість та швидкодію систем захисту інформації.

Список літератури

1. Мухачев В.А. Методи практичної криптографії / В.А. Мухачев, В.А. Хорошко. – К.: ТОВ «Поліграф-Консалтинг», 2005. – 215 с.

2. Алгоритмические основы эллиптической криптографии / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М: Наука, 2004. – 499 стр.

3. Brassard J. Modern Cryptologyy. Springer-Verlag / J. Brassard. – Berlin – Heidelberg, 1988. – 107 p. (Русский перевод: Брассар Ж. Современная криптология. – Полимед, 1999. – 176 с.)

4. Справочная математическая библиотека: Высшая алгебра / Под общей ред. Л.А. Люстерника, А.Р. Янпольского. – М.: Физматгиз, 1962. – 300 с.

5. Рудницький В.М. Моделювання логічних функцій для криптографії на основі перестановок / В.М. Рудницький, Н.М. Пантелєєва // Міжнародна науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2007». Тези доповідей. – Х.: НАКУ «ХАІ», 2007. – С. 209-211.

6. Рудницький В.М. Математичне моделювання дискретних пристроїв для систем інформаційної безпеки / В.М. Рудницький, Н.М. Пантелєєва // Міжнародна науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2007». Тези доповідей. – Х.: НАКУ «ХАІ», 2007. – С. 227-229.

7. Рудницький В.М. Визначення множини логічних функцій для синтезу цифрових пристроїв систем захисту інформації / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко // Системи управління, навігації та зв'язку. – К., ЦНДІ НУ, 2008. – Вип. 4 (8). – С. 155-157.

Надійшла до редколегії 23.01.2009

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Харківський національний технічний університет сільського господарства ім. П. Василенка, Харків.

СИНТЕЗ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ УСТРОЙСТВ ДЕКОДИРОВАНИЯ ИНФОРМАЦИИ ДЛЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

В.М. Рудницкий, В.Г.Бабенко

Работа посвящена разработке теоретических основ построения устройств декодирования на основе синтезированных моделей логических функций специального класса для систем защиты информации. Результаты исследования и математического моделирования экспериментальных данных позволили определить и довести общие закономерности построения функций декодирования на основе использованных функций кодировки.

Ключевые слова: *информационная безопасность, криптография, специализированные логические функции*

SYNTHES OF MATHEMATICAL MODELS OF DEVICES OF DECODING OF INFORMATION FOR THE CRYPTOGRAPHIC SYSTEMS

V.M. Rudnitskiy, V.G.Babenko

Work is devoted a development of theoretical bases of construction of decoding devices on the basis of the synthesized models of specialized boolean functions for the systems of information protection. The results of research and mathematical design of experimental information allowed to define and lead to general conformities to the law of construction of functions of decoding on the basis of the used functions of code.

Keywords: *informative safety, cryptography, boolean functions.*