УДК 004.056

МОДЕЛЮВАННЯ ПРОЦЕСІВ СИНТЕЗУ ЕЛЕМЕНТАРНИХ ЛОГІЧНИХ ФУНКЦІЙ ПІДВИЩЕНОЇ РОЗРЯДНОСТІ

А.В. Ярмілко, Р.Г. Немов

Черкаський національний університет імені Богдана Хмельницького, Україна

За останні кілька десятків років значною мірою було збільшено обсяг та інтенсивність обігу даних у інформаційних системах, і даний процес тільки набирає обертів. Очевидно, що розвитку набувають і методи захисту інформаційних систем від несанкціонованого доступу до даних. Одним із таких методів є крипто-шифрування на основі елементарних логічних функцій. Властивості методу синтезу функцій перестановок, керованих інформацією [1] підтверджують ефективність такого підходу. Тим не менш, для збільшення стійкості інформаційних систем метод крипто-шифрування на основі елементарних логічних функцій потребує постійного розвитку і вдосконалення. Одним із таких шляхів є підвищення розрядності логічних функцій, очікуваним наслідком якого є збільшення стійкості методу за рахунок розширення набору актуальних логічних функцій. Однак, значне зростання кількості елементарних функцій збільшує час їхньої обробки. Тому постає необхідність вирішення задачі модифікації традиційних алгоритмів синтезу елементарних логічних крипто-шифрувальних функцій з метою узгодження їхніх експлуатаційних характеристик з режимами функціонування прикладних інформаційних систем.

Метою дослідження є перевірка ефективності алгоритмів формування оптимальних наборів елементарних функцій за критерієм: часу їх обробки і криптографічної стійкості операцій, сформованих на основі цих функцій.

Для визначення зазначених характеристик було розроблено два алгоритми:

1. Формування наборів елементарних п’ятирозрядних функцій для вибору певного піддіапазону із подальшим синтезом функцій тільки у ньому.

2. Формування наборів елементарних п’ятирозрядних функцій за критерієм достатності у піддіапазонах з нефіксованими межами.

Алгоритм формування наборів елементарних п’ятирозрядних функцій на окремо взятому піддіапазоні із подальшим синтезом функцій тільки у ньому характеризується своєю простотою, оскільки для його реалізації необхідно тільки дані про початкову і кінцеву границі піддіапазону. Однак, даний алгоритм має і свої недоліки,

основним з яких є можливість того, що у вказаному піддіапазоні не буде знайдено потрібну кількість функцій, необхідних для формування криптографічних операцій. Також досить високою є ймовірність випадкового несанкціонованого вибору вказаного піддіапазону.

Мінімізувати зазначені недоліки дозволяє застосування алгоритму формування наборів елементарних логічних крипто-шифрувальних функцій за критерієм достатності у піддіапазонах із нефіксованими межами, описаного у [2]. Ефективність даного алгоритму полягає у можливості формувати набори логічних функцій до того моменту, поки їх не стане достатньо для формування необхідної кількості наборів криптографічних операцій.

У результаті дослідження вказаних алгоритмів встановлено:

1. Час, необхідний для синтезу елементарних логічних функцій у алгоритмі формування п'ятирозрядних наборів елементарних крипто-шифрувальних функцій за критерієм достатності у піддіапазонах з нефіксованими межами, може кардинально змінюватись, оскільки пошук актуальних функцій буде продовжуватись до моменту їх знаходження.

2. Час, необхідний для синтезу елементарних логічних функцій у алгоритмі формування наборів елементарних п'ятирозрядних функцій для вибору певного піддіапазону із подальшим синтезом функцій тільки у ньому, пропорційно залежить від розміру піддіапазону у якому відбувається пошук функцій.

3. Криптографічна стійкість алгоритму формування наборів елементарних п'ятирозрядних функцій для вибору певного піддіапазону із подальшим синтезом функцій тільки у ньому виявилась меншою, ніж у алгоритмі формування наборів елементарних п'ятирозрядних функцій за критерієм достатності у піддіапазонах з нефіксованими межами за рахунок того, що кількість піддіапазонів другого алгоритму зарані невідома і межі піддіапазонів обрані випадковим чином.

Зважаючи на отримані результати дослідження, можна стверджувати, що для подальшого застосування і впровадження ефективніше буде використовувати алгоритм формування наборів елементарних п'ятирозрядних функцій за критерієм достатності у піддіапазонах з нефіксованими межами. Запропонована модифікація базового алгоритму забезпечує можливість використання позитивних наслідків підвищення розрядності логічних функцій у системах з високими динамічними характеристиками інформаційних процесів.

Література

1. Рудницький В. М. Синтез елементарних функцій перестановок, керованих інформацією / В. М. Рудницький, Т. В. Миронюк, О. Г. Мельник, В. П. Щербина // Безпека інформації. – Т. 20, № 3. – К.: НАУ, 2014. – С. 242–247.
2. Немов Р. Г. Модифікація структури процедур вибору та діапазону пошуку логічних крипто-шифрувальних функцій при підвищенні їхньої розрядності / Р. Г. Немов, А. В. Ярмілко // Інформаційні технології в освіті, науці й техніці (ІТОНТ-2018): зб. тез. доп. IV Міжнар. наук.-практ. конф., (Черкаси, 17-18 травня). – Черкаси: ЧДТУ, 2018. – С. 121–123.