ІНФОРМАЦІЙНІ СИСТЕМИ, ОБЧИСЛЮВАЛЬНА Й ЕЛЕКТРОННА ТЕХНІКА, СИСТЕМИ ЗВ'ЯЗКУ ТА ПРИЛАДОБУДУВАННЯ

УДК 004.056.55:004.312.2

[1]В.Г. Бабенко, к.т.н.
[2]Р.П. Мельник, к.т.н.
[2]С.В. Гончар

ОЦІНКА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

[1]Одеська національна академія зв'язку ім. О.С. Попова, e-mail: zolot_verba@rambler.ru
[2]Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України,
e-mail: indigo211212@gmail.com

У статті проведена оцінка ефективності використання матричних та розширених матричних операцій криптографічного перетворення інформації. Наведено приклади розрахунків криптостійкості та коефіцієнтів швидкодії.

Ключові слова: захист інформації, криптографічне перетворення, матричні операції, розширені матричні операції, криптостійкість, коефіцієнт швидкодії.

Постановка проблеми

В даний час все більшого значення набувають технології обробки та передачі великих обсягів даних. При цьому, якщо ці дані становлять таємницю певного рівня, з'являється додаткова вимога до необхідності здійснення захисту таких даних.

Традиційні підходи до розробки засобів криптографічного захисту інформації забезпечують інформаційну безпеку, але при цьому можуть значною мірою впливати на швидкість її обробки та передачі по захищених vpn-каналах і корпоративних мережах передачі даних.

Таким чином, на сьогоднішній день однією з актуальних проблем інформаційної безпеки є розробка швидкодіючих, криптостійких і відносно недорогих апаратно-програмних засобів захисту даних.

Аналіз останніх досліджень

Серед останніх досліджень і публікацій варто виділити: [1, 2], де представлено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації в залежності від складності елементарних функцій та способу перетворення інформації елементарними функціями кожної груп, а також метод синтезу матричних моделей операцій криптографічного перетворення. В роботах [3, 4, 5] була доведена ефективність застосування матричних та розширених матричних операцій для криптографічного перетворення інформації.

Проте в даних дослідженнях не була здійснена оцінка криптостійкості та швидкості реалізації криптографічного захисту інформації. Саме це й робить тему дослідження актуальною.

Формулювання цілей статті

Метою даного дослідження є проведення оцінки криптостійкості та швидкості реалізації криптографічного захисту інформації на основі операцій матричного та розширеного матричного криптографічного перетворення.

Виклад основного матеріалу

Проведемо оцінку ефективності криптографічних алгоритмів на основі розрахунку показників швидкості та криптостійкості.

При проведенні досліджень обмежимося:

- алгоритмами випадкового вибору операцій криптографічного перетворення на основі гамуючої послідовності;
- операціями матричного та розширеного матричного криптографічного перетворення.

Застосуємо метод підвищення швидкості шифрування, сутність якого полягає у використанні гамуючої послідовності як послідовного набору команд виконання випадково вибраної підмножини

операцій криптоперетворення. Необхідно відзначити, що криптостійкість (z) використання цього методу визначається як $z = z_г \cdot z_0$, де $z_г$ – криптостійкість гамуючої послідовності, z_o – криптостійкість операцій криптоперетворення. Кількісна оцінка зміни криптостійкості відносно криптостійкості гамуючої послідовності визначається як $k_z = \frac{z_г \cdot z_0}{z_г} = z_0$.

Криптостійкість і швидкість шифрування (k_v – коефіцієнт швидкодії) визначаються такими параметрами: $K_{mo}(n)$ – кількість матричних операцій вибраної розмірності (n), n_k – розрядність команди виконання послідовностей операцій криптоперетворення, K_{on} – кількість операцій у послідовності, яка реалізує команду.

Підмножина випадково вибраних операцій для даного алгоритму визначається як $П_o = 2^{n_k} \cdot K_{on}$. Кількість випадково вибраних підмножин визначаться як кількість сполучень $K_П = C^{K_{on}}_{K_{mo}(n)}$.

Розглянемо більш детально застосування матричних операцій криптографічного перетворення.

Практична криптостійкість залежить від розрядності пароля $R_П = (2^{n_k} \cdot K_{on}) \log_2(K_{mo}(n))$ і буде пропорційною величині $z_o = 2^{R_П}$.

Наприклад, якщо $n = 4$, $n_k = 4$, а $K_{on} = 4$, тоді $П_o = 64$, $R_П = 64 \cdot \log_2 21840 = 927$ і $z_o = 2^{927}$, що є прийнятним значенням, тому що загальна криптостійкість збільшиться в $1{,}12 \cdot 10^{280}$ разів пропорційно.

Оскільки операції криптоперетворення можуть виконуватися паралельно, то час криптоперетворення буде визначатися лише часом формування n_k розрядів гамуючої послідовності. Тоді коефіцієнт швидкодії буде визначатися відношенням розрядності інформації, яка шифрується на основі операцій криптографічного перетворення під управлінням гамуючої послідовності, до кількості розрядів, над якими виконано гамування: $k_v = \frac{n \cdot K_{on}}{n_k}$.

Коефіцієнт швидкодії для цього прикладу буде $k_v = \frac{n \cdot K_{on}}{n_k} = \frac{4 \cdot 4}{4} = 4$ за умови паралельної реалізації матричних операцій та елементарних функцій.

Зменшити кількість розрядів додаткового пароля можливо за рахунок визначення K_{on} при ініціалізації системи, а в додатковий пароль включати лише перестановки вибраних операцій або перестановки послідовностей операцій, які виконуються відповідно до команд перетворення. Для наведеного прикладу в першому випадку отримаємо: $R_{П1} = 64 \cdot \log_2 64 = 384$ і $z_{o1} = 2^{386} = 3{,}94 \cdot 10^{115}$, в другому випадку отримаємо $R_{П2} = 16 \cdot \log_2 16 = 64$ і $z_{o2} = 2^{64} = 1{,}84 \cdot 10^{20}$.

Наприклад, якщо $n = 3$, $n_k = 3$, а $K_{on} = 3$, тоді $R_П = 24 \cdot \log_2 1344 = 251$ і $z_o = 2^{251}$, що є прийнятним значенням. Коефіцієнт швидкодії для цього прикладу буде $k_v = \frac{n \cdot K_{on}}{n_k} = \frac{3 \cdot 3}{3} = 3$ за умови паралельної реалізації матричних операцій та елементарних функцій.

Наприклад, якщо $n = 4$, $n_k = 5$, а $K_{on} = 6$, тоді $R_П = 192 \cdot \log_2 21840 = 2780$ і $z_o = 2^{2780}$, що є прийнятним значенням. Коефіцієнт швидкодії для цього прикладу буде $k_v = \frac{n \cdot K_{on}}{n_k} = \frac{4 \cdot 6}{5} = 4{,}8$ за умови паралельної реалізації матричних операцій та елементарних функцій.

Вибір параметрів $K_{mo}(n)$, n_k і K_{on} дає можливість забезпечити необхідні значення швидкості шифрування та криптостійкості за рахунок збільшення апаратної та програмної складності реалізації системи криптографічного захисту інформації.

Розроблені методи та засоби криптографічного перетворення забезпечують вирішення важливої науково-технічної задачі підвищення якості функціонування систем захисту інформаційних ресурсів на основі матричного криптографічного перетворення.

Розглянемо застосування розширених матричних операцій криптографічного перетворення.

Проведені дослідження показали ефективність використання методу розширеного матричного

криптографічного перетворення, який забезпечує підвищення криптостійкості закодованої інформації в 2016^{Kc} разів, де Kc – кількість циклів криптографічного перетворення [4]. Ця криптостійкість розраховувалася теоретично, при цьому не враховувалася її залежність від довжини пароля.

Реалізація операцій розширеного матричного криптографічного перетворення відповідає вимогам програмного пакета статистичного тестування NIST STS.

Практичне використання операцій розширеного матричного криптографічного перетворення, виходячи з проведених досліджень, проводиться на основі гамуючої послідовності.

Практична криптостійкість залежить від розрядності пароля $R_{П} = (2^{n_k} \cdot K_{on}) \log_2 2016$ і буде пропорційною величині $z_o = 2^{R_{П}}$.

Наприклад, якщо $n_k = 4$, а $K_{on} = 4$, тоді $П_o = 64$, $R_{П} = 64 \cdot \log_2 2016 = 704$ і $z_o = 2^{704}$, що є прийнятним значенням, тому що загальна криптостійкість збільшиться в 2^{704} разів пропорційно.

Наприклад, якщо $n_k = 4$, а $K_{on} = 2$, тоді $П_o = 32$, $R_{П} = 32 \cdot \log_2 2016 = 352$ і $z_o = 2^{352}$, що є прийнятним значенням, так як загальна криптостійкість збільшиться в 2^{352} разів пропорційно. Для даного прикладу коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{3 \cdot K_{on}}{n_k} = 1{,}5$.

Наприклад, якщо $n_k = 3$, а $K_{on} = 6$, тоді $П_o = 48$, $R_{П} = 48 \cdot \log_2 2016 = 528$ і $z_o = 2^{528}$, що є прийнятним значенням, так як загальна криптостійкість збільшиться в 2^{528} разів пропорційно. Для даного прикладу коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{3 \cdot K_{on}}{n_k} = 6$.

Як видно з прикладів, розширене матричне перетворення залежно від параметрів n_k і K_{on} дає змогу збільшити криптостійкість від 10^{32} до 10^{150} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування від 1,5 до 6 разів.

Висновки

Оцінка якісних показників показала, що використання матричних та розширених матричних операцій криптографічного перетворення забезпечує підвищення криптостійкості та швидкості реалізації алгоритмів криптографічного захисту інформації залежно від задач проектування, що, в свою чергу, дозволяє вирішити важливу науково-технічну задачу підвищення якості систем захисту інформації.

Список літературних джерел

1. Бабенко В. Г. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / В. Г. Бабенко, О. Г. Мельник, Р. П. Мельник // Безпека інформації. – 2013. – Том 19 #1. – С. 56–59.

2. Рудницький В. М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В. М. Рудницький, В. Г. Бабенко, С. В. Рудницький // Збірник наукових праць Харківського університету Повітряних Сил. – 2012. – Вип. 4 (33). – С. 198–200.

3. Рудницкий С. В. Криптографическое преобразование информации на основе трехразрядных логических функций / С. В. Рудницкий, Р. П. Мельник, В. В. Веретельник // Вектор науки Тольяттинского государственного университета. – 2012. – № 4 (22). – С. 119–122.

4. Мельник Р. П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації / Р. П. Мельник // Системи обробки інформації. – 2012. – № 9 (107). – С. 145–147.

5. Криптографическое кодирование: методы и средства реализации (часть 2) : монография / В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко, Р. П. Мельник, С. В. Рудницкий, О. Г. Мельник. – Краснодар, 2014. – 224 с.