в вычислительные системы. Процесс интеграции описан на всех уровнях абстракции: от его модели, описанной на HDL-языке, до драйвера операционной системы. Это позволяет упростить использование такого аппаратного обеспечения конечным пользователем и улучшить применяемость адаптивного подхода к реальным задачам.

Ключевые слова: адаптивное аппаратное обеспечение, вычислительные системы, интеграция с ОС, ускорение вычислений.

Захарченко Тарас Леонідович, *аспірант, кафедра конструювання електронно-обчислювальної апаратури, Національний технічний університет «Київський політехнічний інститут», Україна,* ***e-mail: taras.zakharchenko@gmail.com****.*

Захарченко Тарас Леонидович, *аспирант, кафедра конструирования электронно-вычислительной аппаратуры, Национальный технический университет «Киевский политехнический институт», Украина.*

Zakharchenko Taras, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine,*
e-mail: taras.zakharchenko@gmail.com

УДК 004.056.055
DOI: 10.15587/2312-8372.2015.51221

Миронець І. В.

ПІДВИЩЕННЯ ДОСТОВІРНОСТІ ПРОЦЕСУ МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

Швидкісні криптографічні перетворення даних є найефективнішим засобом забезпечення конфіденційності та цілісності інформаційних ресурсів, тому перспективним напрямком досліджень є розробка методів підвищення продуктивності криптографічних систем.

В статті було сформовано два підходи щодо підвищення достовірності процесу криптографічного перетворення: перший підхід дозволяє проконтролювати корекцію синтезу матриці оберненого перетворення, другий — проконтролювати весь процес проходження оберненого перетворення інформації.

Ключові слова: *криптографічне перетворення, захист інформації, конфіденційність, цілісність інформації, кодування, шифрування інформації.*

1. Вступ

Сучасні методи накопичення, обробки та передачі інформації сприяли появі загроз, пов'язаних з можливістю втрати, розкриття, модифікації даних, що належать кінцевим користувачам.

Використання подібних заходів приводить до необхідності використання комп'ютерів для вирішення специфічних завдань, для вирішення яких необхідна наявність специфічних алгоритмів.

Зважаючи на важливість інформації, яка передається відкритими лініями зв'язку, розрізняють приватну, комерційну, службову та державну таємницю. Враховуючи це, зрозуміло, що таку інформацію потрібно передавати не у відкритому вигляді, а в модифікованому таким чином, щоб перетворити її у відкритий вигляд могла лише особа, що знає необхідне обернене перетворення. Існують два основні способи перетворення даних — кодування та шифрування [1, 2].

Таким чином можна зробити висновок, що захист конфіденційної інформації, що представлена у цифровому вигляді, на сьогоднішній день є достатньо актуальним завданням. Одним із ефективних підходів щодо захисту інформації в комп'ютерних системах є використання криптографічних методів захисту, зокрема блокового шифрування даних.

2. Аналіз літературних даних та постановка проблеми

Для забезпечення конфіденційності та цілісності інформації [3–5] в багатьох випадках криптографічне перетворення є чи не єдиним шляхом (з певною стійкістю до спроб розкриття її змісту — криптографічною стійкістю). На даний час широко відомими є кілька методів криптографічного захисту інформації, серед яких досить важливими є аналітичні матричні перетворення, що розглянуті, наприклад в [3, 4], і до яких відносяться запропоновані авторами в роботах [5, 6] алгоритми криптографічного перетворення [7].

Важливий вклад у розвиток криптології та захисту інформації зробили такі вітчизняні та зарубіжні науковці, як І. Д. Горбенко, А. А. Молдовян, В. А. Мухачев, В. А. Лужецький, В. А. Хорошко, Ю. В. Кузнецов, О. Г. Корченко, Г. Ф. Конахович, Б. Шнайер, М. Хелльман, Ч. Г. Беннет, Ж. Брассар та інші.

Проте залишається цілий ряд невирішених задач, що мають важливе значення. Беручи до уваги те, що швидкісні криптографічні перетворення даних є найефективнішим засобом забезпечення таких характеристик безпеки інформаційних ресурсів, як конфіденційність і цілісність, то, безумовно, перспективним напрямком досліджень є розробка методів підвищення продуктивності криптографічних систем. А саме дане дослідження

базується на підвищенні достовірності результатів криптографічного перетворення.

3. Об'єкт, мета та задачі дослідження

Об'єктом дослідження є процес криптографічного захисту інформаційних ресурсів.

Метою проведення даного дослідження є підвищення достовірності результатів криптографічного перетворення.

Для досягнення поставленої мети необхідно розробити підходи щодо підвищення достовірності процесу криптографічного перетворення.

4. Аналіз синтезу матриць оберненого та взаємного криптографічного перетворення інформації

Запис операцій криптографічного перетворення в дискретно-алгебраїчному представленні дає змогу виявити явні логічні залежності між значеннями розрядів інформації, що беруть участь у процесі криптографічного перетворення інформації.

Крім цього, дискретно-алгебраїчне представлення операцій криптографічного перетворення дає змогу уникнути інваріантності побудови базової групи операцій криптографічного перетворення інформації [8–11].

В загальному вигляді операції криптографічного перетворення, побудовані на основі додавання за модулем два, мають наступний вигляд:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \oplus b_2 \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n \oplus b_n \end{pmatrix}, \quad (1)$$

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; $x_1...x_n$ — операнди-розряди відповідно криптографічного прямого перетворення; $\oplus$ — операція «сума за mod 2» [12].

Тоді процес знаходження операції (матриці) оберненого перетворення матиме наступний вигляд [13]:

$$\vec{F}_d = \begin{pmatrix} b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \end{pmatrix} = \begin{pmatrix} a_{11}x_1 & & & \\ & a_{22}x_2 & & \\ & & . \ . \ . & \\ & & & a_{nn}x_n \end{pmatrix}, \quad (2)$$

або:

$$\vec{F}_d = \begin{pmatrix} b_{11}y_1 \oplus b_{12}y_2 \oplus ... \oplus b_{1n}y_n \\ b_{21}y_1 \oplus b_{22}y_2 \oplus ... \oplus b_{2n}y_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ b_{n1}y_1 \oplus b_{n2}y_2 \oplus ... \oplus b_{nn}y_n \end{pmatrix}, \quad (3)$$

де $x_1...x_n$ — початкові операнди-розряди інформації; $a_{ij} = 1$ при $i = j$, тому що потрібно забезпечити невиродженість перетворення, тобто повинна виконуватись умова $a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \neq 0$, а також відсутні перестановки рядків матриці $b_{ij} \in [0,1]$ — коефіцієнти матриці оберненого перетворення, y_i — операнди-розряди інформації, які отримані в результаті застосування операції прямого перетворення відповідно.

Якщо ж операції криптографічного прямого перетворення без урахування групи операцій інверсії задані виразами:

$$\vec{F}_{k1} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n \end{pmatrix}, \quad (4)$$

де $a_{ij} \in [0,1]$; $x_1...x_n$ — операнди-розряди відповідного криптографічного прямого перетворення; $\oplus$ — операція «сума за mod 2»;

$$\vec{F}_{k2} = \begin{pmatrix} c_{11}x_1 \oplus c_{12}x_2 \oplus ... \oplus c_{1n}x_n \\ c_{21}x_1 \oplus c_{22}x_2 \oplus ... \oplus c_{2n}x_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ c_{n1}x_1 \oplus c_{n2}x_2 \oplus ... \oplus c_{nn}x_n \end{pmatrix}, \quad (5)$$

де $c_{ij} \in [0,1]$; $x_1...x_n$ — операнди-розряди відповідного криптографічного прямого перетворення.

Тоді процес знаходження операції (матриці) взаємного перетворення матиме вигляд [14]:

$$\vec{F}_p = \begin{pmatrix} d_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus d_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ d_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus d_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ d_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus d_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \end{pmatrix} =$$

$$= \begin{pmatrix} c_{11}x_1 \oplus c_{12}x_2 \oplus ... \oplus c_{1n}x_n \\ c_{21}x_1 \oplus c_{22}x_2 \oplus ... \oplus c_{2n}x_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ c_{n1}x_1 \oplus c_{n2}x_2 \oplus ... \oplus c_{nn}x_n \end{pmatrix}, \quad (6)$$

або

$$\vec{F}_p = \begin{pmatrix} d_{11}y_1 \oplus d_{12}y_2 \oplus ... \oplus d_{1n}y_n \\ d_{21}y_1 \oplus d_{22}y_2 \oplus ... \oplus d_{2n}y_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \\ d_{n1}y_1 \oplus d_{n2}y_2 \oplus ... \oplus d_{nn}y_n \end{pmatrix}, \quad (7)$$

де $d_{ij} \in [0,1]$; $x_1...x_n$ — операнди-розряди відповідно.

5. Розробка підходів щодо підвищення достовірності процесу криптографічного перетворення

Отримані операції (2) та (5) повинні приводити до одного і того ж результату, тому можемо зробити висновок, що $\vec{F}_d = \vec{F}_p$, тобто відповідні операнди-розряди є рівними $b_{ij} = d_{ij}$, причому $b_{ij} \in [0,1]$, $d_{ij} \in [0,1]$. Даний підхід дозволяє проконтролювати корекцію синтезу

матриці оберненого перетворення, оскільки отримали рівність $\vec{F}_d = \vec{F}_p$.

Іншим підходом щодо підвищення достовірності процесу криптографічного перетворення можна вважати підхід, коли знаходження операції (матриці) оберненого перетворення має вигляд (3), а операцію криптографічного прямого перетворення для проведення взаємного перетворення задати як:

$$\vec{F}_k(x_i) * \vec{F}_{per}(x_i),$$

де $\vec{F}_k(x_i)$ — операції прямого криптографічного перетворення, $\vec{F}_{per}(x_i)$ — матриця перестановок.

Тоді отримані операції взаємного перетворення (7) та операції оберненого перетворення (3) не співпадатимуть, тобто матимуть різні алгоритми процесу перетворення інформації $\vec{F}_d \neq \vec{F}_p$, так як $b_{ij} \neq d_{ij}$, причому $b_{ij} \in [0,1]$, $d_{ij} \in [0,1]$. Проте при рішенні $\vec{F}_d$ та $\vec{F}_p$ буде отримано один і той же результат.

Такий підхід дозволяє проконтролювати весь процес проходження оберненого перетворення інформації, а саме знаходження оберненої матриці та результати декодування.

6. Висновки

У результаті проведених досліджень було сформовано два підходи щодо підвищення достовірності процесу криптографічного перетворення.

Перший підхід дозволяє проконтролювати корекцію синтезу матриці оберненого перетворення інформації. Другий підхід дозволяє проконтролювати весь процес проходження оберненого перетворення інформації, а саме знаходження оберненої матриці та результати декодування.

Література

1. Рудницький, В. М. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів [Текст]: зб. наук. пр. / В. М. Рудницький, І. В. Миронець, В. Г. Бабенко // Системи обробки інформації. — Х.: Харк. ун-т Повітряних Сил ім. Івана Кожедуба, 2010. — Вип. 5(86). — С. 15–19.
2. Рудницький, В. М. Обґрунтування можливості розширення набору функцій перекодування інформації для захисту конфіденційних інформаційних ресурсів [Текст]: зб. наук. пр. / В. М. Рудницький, І. В. Миронець, В. Г. Бабенко // Системи управління, навігації та зв'язку. — Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2010. — Вип. 2(14). — С. 118–122.
3. Чипига, А. Ф. Информационная безопасность автоматизированных систем [Текст]: учеб. пособ. для студ. вузов / А. Ф. Чипига. — М.: Гелиос АРВ, 2010. — 336 с.
4. Ростовцев, А. Г. Теоретическая криптография [Текст] / А. Г. Ростовцев, Е. Б. Маховенко. — М.: Профессионал, 2005. — 490 с.
5. Василенко, В. С. Варіант завадостійкості криптографічного перетворення [Текст] / В. С. Василенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації Україні. — 2004. — Вип. 8. — С. 101–108.
6. Матов, О. Я. Матричні завадостійкі криптографічні перетворення [Текст] / О. Я. Матов, М. Ю. Василенко // Реєстрація, зберігання і обробка даних. — 2011. — Т. 13, № 4. — С. 39–51.
7. Матов, О. Я. Криптозахист інформаційних об'єктів шляхом блокових перетворень із системи лишкових класів у позиційну систему числення [Текст] / О. Я. Матов, В. С. Василенко, М. Ю. Василенко // Реєстрація, зберігання і обробка даних. — 2012. — Т. 14, № 3. — С. 99–103.
8. Goldreich, O. Foundations of Cryptography [Text]. Volume 1. Basic Tools / O. Goldreich. — Cambridge, United Kingdom: Cambridge University Press, 2001. — 396 p. doi:10.1017/cbo9780511546891
9. Goldreich, O. Foundations of Cryptography [Text]. Volume 2. Basic Applications / O. Goldreich. — Cambridge, United Kingdom: Cambridge University Press, 2004. — 452 p. doi:10.1017/cbo9780511721656
10. Koblitz, N. Algebraic Aspects of Cryptography [Text] / N. Koblitz. — Berlin: Springer-Verlag, 1998. — 206 p. doi:10.1007/978-3-662-03642-6
11. Menezes, A. Handbook of Applied Cryptography [Text] / A. Menezes, P. van Oorschot, S. Vanstone // Discrete Mathematics and Its Applications. — CRC Press, 1996. — 780 p. doi:10.1201/9781439821916
12. Голуб, С. В. Вдосконалення методу синтезу операцій криптографічного перетворення на основі дискретно-алгебраїчного представлення операцій [Текст]: зб. наук. праць / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький, Р. П. Мельник // Системи управління, навігації та зв'язку. — К.: Центр. наук.-досл. ін-т навігації і управл., 2012. — Вип. 2(22). — С. 163–168.
13. Рудницький, В. М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації [Текст]: зб. наук. праць / В. М. Рудницький, В. Г. Бабенко, С. В. Рудницький. — Х.: ХУПС ім. І. Кожедуба, 2012. — Вип. 4(33). — С. 198–200.
14. Рудницький, В. М. Метод синтезу матричних моделей операцій криптографічного перекодування інформації [Текст]: наук.-практ. журн. / В. М. Рудницький, В. Г. Бабенко, С. В. Рудницький // Захист інформації. — К.: НАУ, 2012. — № 3(56). — С. 50–56.

ПОВЫШЕНИЕ ДОСТОВЕРНОСТИ ПРОЦЕССА МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

Скоростные криптографические преобразования данных являются эффективным средством обеспечения конфиденциальности и целостности информационных ресурсов, поэтому перспективным направлением исследований является разработка методов повышения производительности криптографических систем.

В статье было сформировано два подхода по повышению достоверности процесса криптографического преобразования: первый подход позволяет проконтролировать коррекцию синтеза матрицы обратного преобразования, второй — проконтролировать весь процесс прохождения обратного преобразования информации.

Ключевые слова: криптографическое преобразование, защита информации, конфиденциальность, целостность информации, кодирование, шифрование информации.

Миронець Ірина Валеріївна, *кандидат технічних наук, доцент, кафедра інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Україна,* ***e-mail: irenmir@ukr.net****.*

Миронец Ирина Валериевна, *кандидат технических наук, доцент, кафедра информационной безопасности и компьютерной инженерии, Черкасский государственный технологический университет, Украина.*

Mironets Irina, *Cherkasy State Technological University, Ukraine,* ***e-mail: irenmir@ukr.net***