Рисунок 1 – Приклад муарового зображення

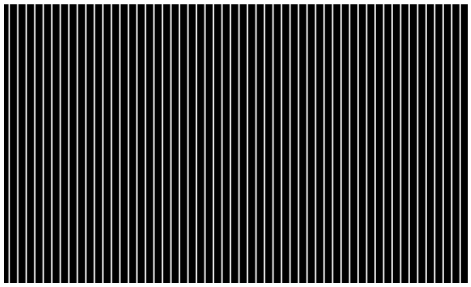

Рисунок 2 –Приклад виконання базового шару

Даний приклад показує, як виконано захист в елементі захисного елементу. Отримано базовий шар, який показано на рис.2, який складається з паралельних ліній, а також основний об'єкт, який зображено на рис.1. основний об'єкт включає в себе 4 накладених шари, які побудовані за допомогою паралельних ліній, зміщених на певний період від базового шару. Таким чином отримуємо об'єкт з декількох шарів, які перетинаються та накладаються в певних проміжках об'єкту, за рахунок чого отримаємо муар на цих перетинах, якщо відбудеться фальсифікація документу і приховане зображення стане явним з муаром.

Висновки

Для захисту інформації запропоновано метод побудови латентних елементів, який має надійний захист при копіюванні оригінального документу. При розробці використано PDF-формат, що забезпечує високу якість друку захищених документів. Роботу методу проілюстровано прикладами. Запропонований метод може бути використаний для захисту друкованої інформації, документів звітності та документів державного зразку. Розроблено метод захисту документів, що дозволяє побудувати приховані елементи з використанням ефекту муару. для побудови застосовані паралельні структури з різними кутами нахил. метод створює візуальний ефект руху зображення. В результаті використання методу рівень захисту документів значно підвищується.

Список використаних джерел

1. Дронюк І. Розробка методу захисту цінних паперів на стадії додрукарської підготовки / І. Дронюк, М. Назаркевич, О. Миронюк //Вісник Національного університету «Львівська політехніка». Комп' ютерні науки та інформаційні технології. - 2011. - № 694. - С. 352-358.
2. Nazarkevych M.A. The development of software for the protection of printed documents / M. Nazarkevych, O.Troyan // Proceedings of the international scientific-practical. Conf. ITSEC
3. Maria Nazarkevych Analysis of Software Protection and Development of Methods of Latency in Printed Documents /Maria Nazarkevych, Oksana Troyan // In Proc. of the VIIIth International Scientific and Technical Conference CSIT 2013, 16-18 November, Lviv 2013, p.120-121.
4. Nazarkevych M.A. Analysis of modern methods and software items with graphic printed documents protection / Maria Nazarkevych Oksana Trojan // Technical news. - 2013. № 1 (37). - S. 42 - 44.
5. Киппхан Г. Энциклопедия по печатным средствам информации. Технологии и способы производства / Перевод с немецкого — М.: МГУП, 2003. – 1280 с. 2. Мандельброт Б. Фракталы, случай и финансы / Б. Мандельброт. — Москва-Ижевск: Регулярная и хаотическая динамика, 2004. — 256 с.

УДК 683.1

АНАЛІЗ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ З ВИКОРИСТАННЯМ МАСКОВАНОГО ПРЕДСТАВЛЕННЯ ДАНИХ

Якименко І.З. [1)], Божик С.В. [2)]

Тернопільський національний економічний університет

[1)] к.т.н., доцент; [2)] магістрант

І. Постановка проблеми

При зростанні цінності інформаційних потоків в комп'ютерних мережах, які зберігаються, обробляються та передаються зумовлює зростання задач забезпечення конфіденційності, цілісності та автентичності інформації при зростанні ймовірності реалізації загроз несанкціонованого доступу до такої інформації [1–3]. Класично у комп'ютерних системах вирішення розглянутих задач розв'язують

з допомогою криптографічних методів перетворення інформації. Сучасні криптографічні перетворення забезпечують необхідний рівень захисту інформаційних потоків стійких до інженерно-криптографічних атак до математичного аналізу з метою обчислення основних параметрів криптоперетворень.

З аналізу праць П. Кочера, Т. Мессергеса [4-5] випливає, що використання "маскованого представлення" в результаті побудови арифметичних та логічних методів обробки даних, дозволяє будувати комп'ютерні компоненти на базі традиційної елементної бази, які володіють підвищеною стійкістю до атак на основі енергоспоживання та низькою вартістю виготовлення.

II. Мета роботи.

Робота присвячена аналізу ефективності захисту інформаційних потоків в комп'ютерних мережах на основі криптографічних перетворень, з використанням маскованого представлення даних.

III. Масковане представлення даних для базових операцій алгоритмів криптографічних перетворень

Аналіз алгоритмів криптографічних перетворень, проведений у [6], показав, що структура та набір базових операцій алгоритмів криптографічних перетворень залежить від вибору рівня абстракції представлення цих алгоритмів. До найбільш поширених елементарних базових операцій входять: логічні операції булевої алгебри логіки над двійковим представленням даних – логічне множення (кон'юнкція), логічне додавання (диз'юнкція), логічне заперечення та, додатково, операція еквівалентності (додавання за модулем два); операції маніпулювання бітами – перестановки бітів та циклічні зсуви; операції додавання у скінчених кільцях; операції додавання, множення та пошуку оберненого елемента у скінчених полях Галуа з характеристикою 2; операції заміни одного елемента даних на інший за допомогою таблиці.

Виконання перелічених операцій над даними у маскованому представленні не є тривіальним та, загалом, потребує модифікування алгоритмів виконання цих базових операцій [7]. Слід зазначити, що модифікування на алгоритмічному рівні визнано найдоцільнішим з точки зору вартості реалізації та стійкості проти інженерно-криптографічних атак. При цьому, виникає актуальна задача адаптування відомих алгоритмів криптографічних перетворень до обробки інформації у маскованому представленні. Для вирішення даного класу задач необхідно розробити нові алгоритми з врахуванням обробки маскованих даних, які дозволяють отримувати аналогічні результати до початкових, в тому числі з використанням немаскованих даних.

Традиційний спосіб виконання арифметичних операцій над даними у маскованому представленні з логічною маскою полягає у послідовному виконання таких перетворень [8]: перетворення маскованого представлення даних із логічним маскуванням у представлення з арифметичним маскуванням; виконання арифметичної операції над даними з арифметичною маскою; обчислення/генерування нової арифметичної маски; перетворення маскованого представлення даних із арифметичним маскуванням у представлення з логічним маскуванням.

Однак, недоліком такого способу обробки даних є його висока часова складність, оскільки необхідно використовувати чотири послідовні перетворення, що призводить до зменшення продуктивності обробки даних.

Тому перспективним напрямком дослідження є розробка методів виконання арифметичних операцій та перетворення маскованого представлення даних, які є масштабованими до розрядності масок та володіти при цьому низькою місткістною складністю.

IV. Висновок

Проведений аналіз ефективності захисту інформаційних потоків в комп'ютерних мережах на основі криптографічних перетворень, з використанням маскованого представлення даних та встановлено переваги та недоліки даного підходу.

Список використаних джерел

1. Закон України "Про захист інформації в автоматизованих системах" від 05.07.1994
2. Згуровський М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2000. – С. 10 – 14.
3. Концепція технічного захисту інформації в Україні. Затверджена постановою Кабінету Міністрів України від 8 жовтня 1997 р., № 1126.
4. Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems // Lecture Notes in Computer Science: Proc. of International Conf. Advances in Cryptology. CRYPTO-1996. – Berlin: Springer, 1996. – Vol. 1109. – P. 104-113.
5. Kocher P., Jaffe J., Jun B. Using unpredictable information to minimize leakage from smartcards and other cryptosystems // USA Patent, International Publication. – 1999. – WO 99/63696.

6. Коркішко Т.А., Мельник А. О., Мельник В.А. Захист інформації в комп'ютерних і телекомунікаційних мережах: Алгоритми та процесори симетричного блокового шифрування. Львів: БАК, 2003. – 168 с.
7. Karpinskyy M., Korkishko L. Architecture of cryptographic devices resistant to side-channel attacks // Proc. of the International Conf. on Computer Science and Information Technologies. CSIT-2006. – Lviv: Lviv Polytechnic National University,2006. – P. 167-170.
8. Golic J., Tymen Ch. Multiplicative masking and power analysis of for AES // Lecture Notes in Computer Science: Proc. of International workshop Cryptographic Hardware and Embedded Systems. CHES 2002. – Berlin: Springer, 2002. – Vol. 2523. – P. 198-212.

УДК 681.3

МЕТОД ФАКТОРИЗАЦІЇ ЧИСЕЛ ВЕЛИКОЇ РОЗРЯДНОСТІ НА ОСНОВІ ТЧБ РАДЕМАХЕРА-КРЕСТЕНСОНА

Якименко І.З.[1)], **Івасьєв С.В,**[2)], **Назаров В.І.** [3)]
Тернопільський національний економічний університет
[1)] *к.т.н., доцент;* [2)] *аспірант;* [2)] *магістрант*

I. Постановка проблеми

Факторизацією натурального числа називається його розкладання в добуток простих множників. Це завдання має велику обчислювальну складність. Один з найпопулярніших методів криптографії з відкритим ключем, метод RSA, заснований на трудомісткості завдання факторизації довгих цілих чисел [1].

II. Мета роботи

Метою роботи є модифікація методу факторизації Ферма для оцінки криптостійкості RSA-подібних асиметричних шифрів в криптографічних системах захисту інформації, зменшення складності та підвищення швидкодії алгоритмів.

III. Удосконалений алгоритм Ферма

В даному методі Ферма доцільно скористатися теоретико-числовим базисом Крестенсона [2], який дозволяє зменшити обчислювальну складність за рахунок зменшення розрядностей чисел, над якими проводяться операції.

Тобто в рівнянні:

$$x^2 = y^2 - n \tag{1}$$

робимо наступне перетворення:

$$x^2 mod\ p = y^2 - n\ mod\ p, \tag{2}$$

в результаті отримали $x^2 \equiv (y^2 - n) mod\ p$

Для рішення даного порівняння доцільно скористатися символами Якобі, які дозволяють однозначно вказувати, чи обчислюється корінь за модулем.

Нехай p – просте, a – ціле число. Символ Лежандра $\left(\frac{a}{p}\right)$ визначається так:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ якщо } p \text{ ділиться на } a \\ 1, \text{ якщо } a \in Q_p \\ -1, \text{ якщо } a \in \bar{Q}_p \end{cases}.$$

Число a, яке не ділиться на непарне просте p, є квадратичним лишком за модулем p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, і квадратичним нелишком тоді і тільки тоді коли $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

За теоремою Ферма [1, 2] ap-1 ≡ 1 (mod p) при НСД(a, p) = 1 та НСД(2, p) = 1. Або:

$$\left(a^{\frac{p-1}{2}} + 1\right) * \left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \bmod p.$$

Звідси вираз в одній із дужок ділиться на p. Обидві дужки не можуть ділитися на p, оскільки тоді на p ділилася б і їх різниця, яка дорівнює 2, а за умовою теореми p – непарне просте число. Якщо a є квадратичним лишком, то a = x2 (mod p) для деякого такого x, що НСД(x, p) = 1. Маємо: