Odessa National Marine University
Kharkov National University of Radio Electronics
Odessa National Polytechnic University
Admiral S.O. Makarov National University of Shipbuilding
Lodz University of Technology

MATERIALS
OF THE VI INTERNATIONAL
SCIENTIFIC- PRACTICAL CONFERENCE

«Information Control Systems and Technologies»
20th – 22th September, 2017

Odessa
2017

модельным временем; модуль управления процессами модели в зависимости от происходящих событий; модуль сбора и оценки информации. Предлагаемая модель позволяет:

1. Проследить динамику восстановления работоспособности СОТС для различных сценариев и систем диагностики.
2. Оценить эффективность системы диагностики с точки зрения изменения времени восстановления работоспособности СОТС и с учетом наступления вторичных последствий.
3. Оценить эффективность внедрения тех или иных организационно-технических мер с точки зрения затрат времени на диагностику, поддержание и восстановление работоспособности конкретных СОТС.

Литература

[1] Черкесов Г.Н. Методы и модели оценки живучести сложных систем / Г.Н. Черкесов. – Москва: «Знание», 1987. – 32 с.

[2] Risk management : principles and guidelines: ISO 31000:2009 — Geneva: International Organization for Standardization, 2009. – 29 p.

УДК 004.056.55

К.т.н. Красиленко В.Г., Нікітович Д.В.

ВДОСКОНАЛЕННЯ ТА МОДЕЛЮВАННЯ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ МАТРИЧНОГО ТИПУ ДЛЯ ТЕКСТОГРАФІЧНИХ ДОКУМЕНТІВ

Ph.D. Krasilenko V.G., Nikitovich D.V.

IMPROVEMENT AND MODELING OF ELECTRONIC DIGITAL SIGNATURES OF MATRIX TYPE FOR TEXTOGRAPHIC DOCUMENTS

Вступ. В епоху електронних комунікацій великі масиви різноманітних текстографічних документів (ТГД) у вигляді цифрових, табличних даних, малюнків, графіків, діаграм, підписів, віз, резолюцій, що є по суті 2-D масивами (зображеннями), необхідно передавати як звітність у податкові та інші державні органи та засвідчувати їх електронним цифровим підписом (ЕЦП).

З урахуванням збільшення сфер застосувань ЕЦП, вимог до них, в тому числі до їх криптостійкості, актуальним завданням є вдосконалення та покращення показників існуючих методів та засобів створення ЕЦП.

Аналіз останніх досліджень і публікацій.

Існує низка класичних ЕЦП, таких як ЕЦП на основі RSA та з хешуванням ТГД, Ель-Гамаля, Шнорра, DSA, незаперечні підписи, сліпі підписи та інші.

Але більшість відомих алгоритмів та протоколів створення ЕЦП, протоколів формування ключів та систем верифікації ЕЦП орієнтовані на послідовну скалярну обробку блоків ТГД, перетворених у цифрові формати.

В [1] були запропоновані матричні моделі (ММ), а в [2] модифікації системи RSA на матричний випадок, які пізніше були використані і для створення ЕЦП для любих ТГД.

У роботі [3] розроблені, досліджені і промодельовані цифрові сліпі підписи на основі матричних афінних шифрів, а в [4] - ЕЦП МТ (матричного типу) для ТГД на базі модифікацій алгоритму RSA МТ і Ель-Гамаля до МТ та продемонстровані їх можливості та переваги.

Але в [4] наводилися результати моделювання таких ЕЦП МТ лише для невеликих масивів чорно-білих зображень розмірністю 128×128 елементів. Постановка задачі.

Тому метою даної роботи є подальше вдосконалення, дослідження ММ при створенні ЕЦП МТ та перевірка їх функціональних можливостей і переваг шляхом моделювання у середовищі Mathcad на конкретних ТГД з демонстрацією утворених ЕЦП МТ.

Це дозволить оцінити якість ММ та показники таких ЕЦП МТ, їх особливості і сфери застосувань.

Виклад основного матеріалу та результатів дослідження. Спочатку ми зробимо короткий огляд існуючих ЕЦП скалярного типу (СТ) та відомих ЕЦП МТ.

Ідея модифікацій класичних ЕЦП СТ до МТ базується на узагальненні базового скалярного RSA до відповідної ММ [2, 4], коли в якості ключів вибираються не скаляри, а відповідні матриці KEY(E) та KEY(D).

Для цього вибирається таких два простих числа k та l або дві матриці K та L з елементами попарно простих чисел k_i,j та l_i,j , таких щоб їх добуток n_i,j трохи перевищував значення елемента масиву, що підлягає зашифруванню і представлений байтом або трьома байтами для кольорового формату.

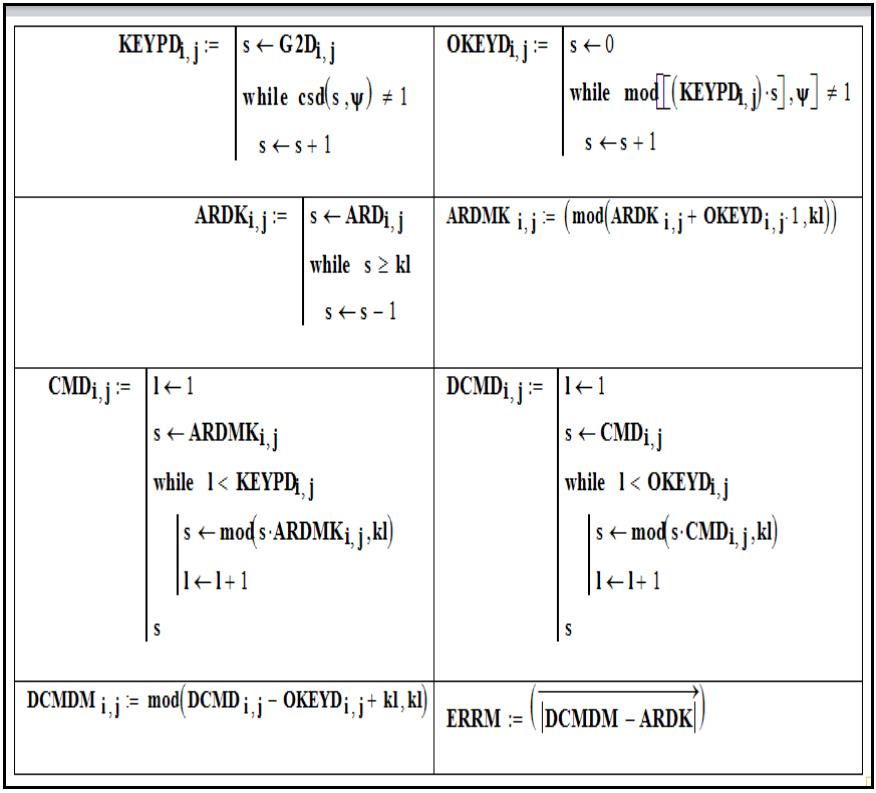

Рис.1 Формули, що використовувались для моделювання ЕЦП RSA MT

Ключі формуються як матриці, кожен елемент яких вибирається з множини значень відповідних скалярних ключів e_i,j та d_i,j, тобто значення елементів KEY(E)_i,j та KEY(D)_i,j матричних ключів KEY(E) та KEY(D) вибираються з множини взаємно простих чисел, що задається

відповідною функцією Ейлера від n_i,j, яка і визначає потужність цієї множини.

Потужність множини ключів залежить як від потужності множини допустимих значень для кожного елемента так і від загальної кількості елементів у 2-D масиві. А це при значних розмінностях масивів дає прийнятні високі оцінки.

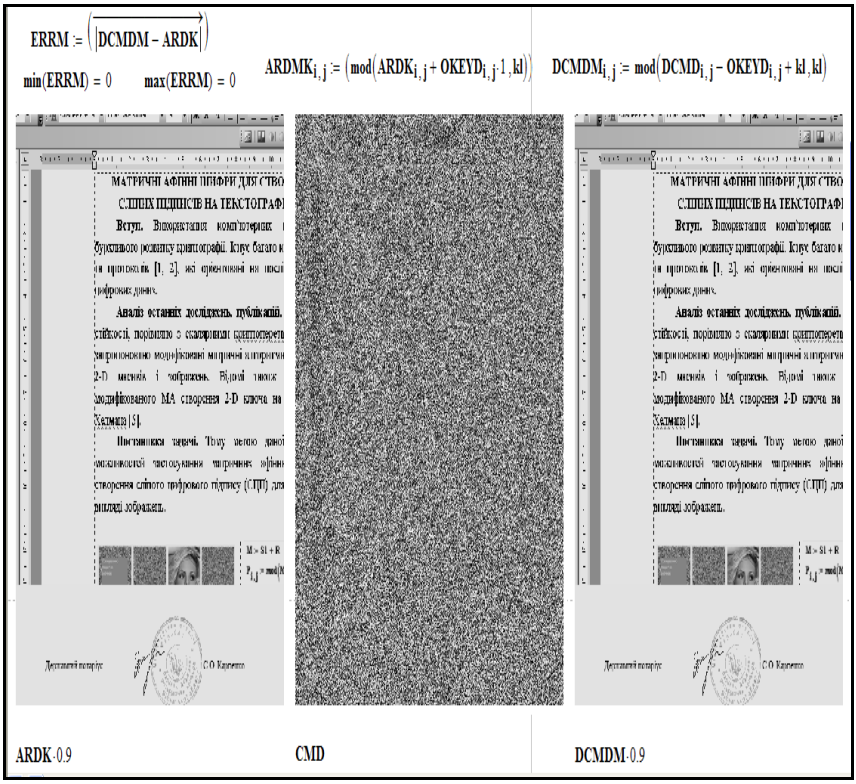

Рис.2 Результати моделювання ЕЦП МТ: ТГД, його ЕЦП і верифікований ТГД

Елементи ЕЦП (EDS) на базі RSA МТ для масиву ТГД, що представлений матрицею T, обчислюються першою стороною при використанні приватного ключа KEY(D) (його елементів d_i,j)

поелементно-матричним піднесенням у степінь за відповідними модулями (ПЕМПуСМ) за формулою: EDS_i,j ≡ T_i,j^d_i,j mod n_i,j.

Утворений ЕЦП разом з Т сторона пересилає другій стороні, яка для верифікації ЕЦП, використовуючи публічний ключ KEY(E), обчислює TV_i,j ≡ EDS_i,j^e_i,j mod n_i,j та порівнює з Т.

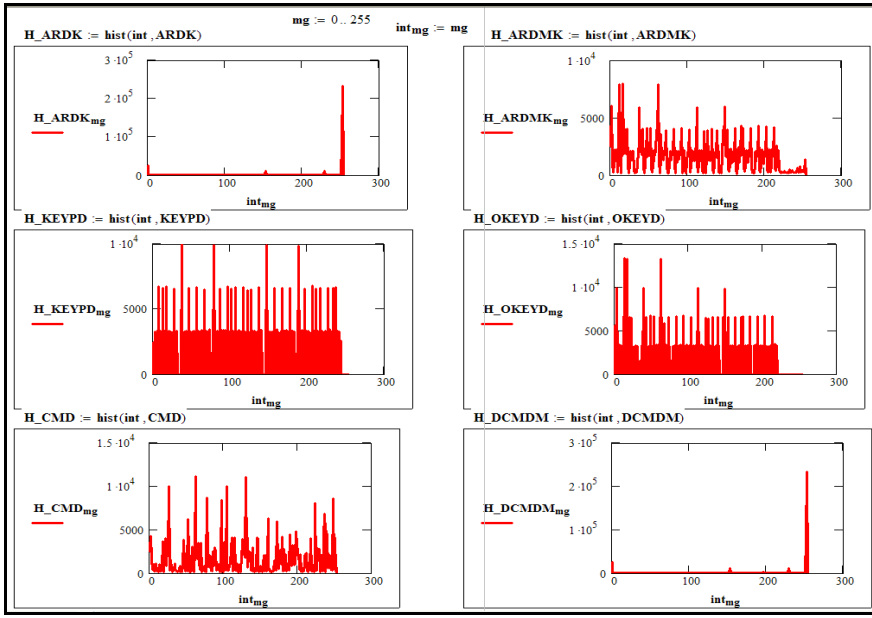

Рис.3 Результати гістограмного аналізу якості покращеного ЕЦП МТ для ТГД

Тут ми, на відміну від робіт [2,4], пропонуємо для покращення стійкості ЕЦП, вищевказану процедуру ПЕМПуСМ повторити певну кількість разів, як стороні першій так і другій з тими ж ключами, утворюючи чергові нові ЕЦП (чи TV) з утворених на попередніх кроках. Тому такий вдосконалений ЕЦП назвемо багатокроковим ЕЦП RSA МТ.

Відомо, що не існує жодного ефективного алгоритму розв'язування задачі обчислення дискретного логарифма за модулем , а тому поряд з розширенням і ускладненням задачі на матричний випадок, особливо за рахунок збільшення потужностей множин матричних ключів та матриць-

модулів, введення багатокрокової ММ призводить до ще більш складнішого розв'язування вище вказаної задачі.

Але, як показали деякі виконані нами модельні експерименти, для деяких видів ТГД зі значними фрагментами з близькими (рівними) значеннями яскравості елементів навіть багатокрокова ММ не задовольняє вимог. Ці демонстраційні приклади тут з урахуванням обмежень не наводяться. А тому друге наше вдосконалення полягає у додатковому закритті ТГД публічним ключем KEY(E) (в експериментах та OKEYD) перед процедурою ПЕМПуСМ першою стороною та додатковим відкриттям цим же ключем після зворотної процедури ПЕМПуСМ другою стороною при перевірці ЕЦП МТ. Це значно поліпшує якість та гістограмно-ентропійні характеристики таких покращених ЕЦП. На рис.1-3 показані результати моделювання процесів створення ЕЦП для ТГД формату А4 (704*572 ел.), що підтверджують адекватність ММ. Питання узгодження матричних ключів були розглянуті у низці наших попередніх робіт, включаючи [5], а тому тут не розглядаються.

Література

[1] Красиленко В. Г. Моделювання матричних алгоритмів криптографічного захисту / В. Г. Красиленко, Ю. А. Флавицька // Вісн. нац. ун-ту "Львів. політехнік", 2009. – № 658. – С. 59 – 63.

[2] Красиленко В. Г. Модифікації системи RSA для створення на її основі матричних моделей та алгоритмів для зашифрування та розшифрування зображень / В.Г. Красиленко, С. К. Грабовляк // Системи обробки інформації, 2012. – №8(106). – С.102 –106.

[3] Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60 – 63.

[4] Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей матричного типу / В.Г. Красиленко, Р. О. Яцковська, Ю. М.

Тріфонова, // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 3(110). – Т. 2. – С. 18 – 22.

[5] Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи обробки інформації. – Х.: ХУПС, 2017. – Вип. 3 (149). – С 151 – 157.

УДК 005.8: 004.02

Ph.D. Grigorian T.G.

MATHEMATICAL MODEL OF PROJECT PARTICIPANTS VALUES HARMONIZATION (STAKEHOLDERS' INTERESTS MAXIMIZATION)

Today the value becomes a key driver for project initiation, implementation and finalization. One of the most important tasks in ensuring of value creation and delivering is its harmonization [1]. The reason to solve the value harmonization problem is a conflict of interests between project participants due to the difference in values and perceptions of the project and its output. The goal of stakeholders' value harmonization is to ensure the stakeholders support during project implementation and, ultimately, the adoption of a product, aimed at creating and delivering value. Thus, there is a need for models that will help us to develop most effective models of project manager behavior in certain situations.

Taking into account the value, processes of its management and project management features, it is most expedient to use harmonization of project works in accordance with stakeholders' values on the basis of non-cooperative matrix games theory [2]. It is due to the absence of strict opposition in stakeholder interests i.e. the conflict is not strictly antagonistic. We will single project participants into two players: A – a sponsor with customers of a product and B – a project manager with his team. Players A and B have m and n strategies respectively: A_1, A_2, ..., A_m and B_1, B_2, ..., B_n. In general case payoffs of players A and B are given by matrices $\mathbf{A} = [a_{ij}]_{m \times n}$ and