

Marma-Crypto: Протокол криптографічно-геометричного водяного знака та суверенного запечатування документів на основі нелінійної планіметрії Шрі Янтри та еліптичних кривих над $GF(2^{257})$ (ДСТУ 4145-2002)

Ярослав Володимирович Баєнко (Yaroslav V. Baienko)

Адвокат, дослідник прикладної криптографії та правової інженерії (Україна, м. Одеса / м. Київ)

Електронна пошта: zerhug@gmail.com · Кваліфікований сертифікат X.509:

10FF6F932221FA00CB44070000000000130616768

Відбиток ключа OpenPGP (RSA-4096): 3D5A ACFD E32C 98FE 8819 9D47 D2A2 C1C4 9164 673B · CERN Zenodo

DOI: 10.5281/zenodo.23429018

Анотація (Abstract)

Суто математична система верифікації цілісності документів повинна дозволяти автору нерозривно пов'язати зміст тексту з видимою векторною геометрією печатки без залучення централізованих серверів перевірки, растрового шуму чи декоративних візуальних штампів. Традиційні цифрові підписи відокремлюють бінарний контейнер CMS / PKCS#7 (IETF RFC 5652) від візуального образу сторінки, тоді як растрові водяні знаки руйнуються при масштабуванні та векторній конвертації. У цій роботі запропоновано протокол **Marma-Crypto** — двоконтурну криптографічно-геометричну систему, яка детерміновано відображає вектор цифрового підпису (r, s) еліптичної кривої над скінченним полем Галуа характеристики два $GF(2^{257})$ згідно з національним стандартом України ДСТУ 4145-2002 (при гешуванні за ДСТУ ГОСТ 34.311-95, ДСТУ 7564:2014 «Купина» та FIPS 180-4 SHA-256) через 24-бітний поблочний квантувальник безпосередньо у мікро-збурення координат $\delta_k \in [-10^{-5}, +10^{-5}]$ дев'яти взаємопов'язаних трикутників класичної планіметричної діаграми Шрі Янтри (**Nava-Cakra**). Завдяки нелінійній зв'язаності 54 потрібних перетинів (**марм**), точному збереженню аналітичного інваріанта білатеральної симетрії $lx_k + rx_k = 2C_x$ та вбудовуванню довгострокового контейнера ETSI EN 319 142-1 (PAdES-B-LTA) із кваліфікованою позначкою часу RFC 3161 TSP і сховищем безпеки /DSS (ISO 32000-2), запропонований водяний знак залишається оптично невідрізним від канонічного архетипу, але забезпечує публічну безключову верифікацію та детерміноване виявлення зміни хоча б одного байта тексту або зміщення вершин понад 10^{-7} координатних одиниць.

1. Вступ та постановка науково-технічної проблеми

Автентифікація електронних документів у судочинстві, міжнародному комерційному арбітражі, інженерії та охороні об'єктів інтелектуальної власності спирається на два історично роз'єднані механізми: бінарні криптографічні контейнери (IETF RFC 5652 CMS, ETSI EN 319 122 CAdES, ETSI EN 319 142 PAdES) та візуальні водяні знаки. Розглянутий окремо, кожен із цих механізмів має фундаментальне структурне обмеження.

По-перше, стандартні кваліфіковані електронні підписи (КЕП / EU eIDAS QES) існують як прихована ASN.1 DER-структура у потоці файлу. Візуальна позначка на сторінці PDF (прямокутна плашка або растровий QR-код) є лише декоративною анотацією: геометричні координати ліній цього штампа не несуть криптографічної ентропії й не пов'язані алгебраїчними рівняннями з дайджестом документа.



По-друге, класична цифрова стеганографія (модифікація найменш значущих бітів LSB у растрових матрицях, частотна модуляція ДКП/вейвлетів або періодичні гільйошні сітки Ліссажу) розрахована на піксельні растри або офсетний банкетний друк. При роботі з сучасними векторними форматами (ISO 32000-2 .pdf, W3C .svg, ISO/IEC 29500 .docx, кресленнями CAD) растрові збурення або зникають під час векторного рендерингу, або порушують типографічну чистоту документа.

Формулюється така наукова задача: **чи можливо побудувати замкнену планіметричну конфігурацію високої алгебраїчної зв'язаності, у якій координати вершин векторних полігонів з рухомою комою одночасно задовольняють жорсткій системі нелінійних геометричних інваріантів і бієктивно кодують вектор підпису (r, s) еліптичної кривої ДСТУ 4145-2002 від нормалізованого змісту документа з можливістю публічної безключової перевірки?**

У цій роботі доведено, що нелінійна дев'ятитрикутна конфігурація **Шрі Янтри** (аналітично досліджена А. П. Кулаїчевим, 1984 [1]), поєднана з арифметикою еліптичних кривих над бінарним полем Галуа $\text{GF}(2^{257})$, дає точний математичний розв'язок поставленої задачі.

2. Нелінійна планіметрична система 9 трикутників Шрі Янтри

Геометричне ядро діаграми Шрі Янтри (**Nava-Cakra**) утворене взаємним перетином дев'яти головних рівнобедрених трикутників, вписаних у коло радіуса $R_0 = \lambda \cdot 100$ із центром на осі симетрії $C_x = \lambda \cdot 150$ у канонічному просторі $[0, 2C_x]^2$ (де масштабний коефіцієнт $\lambda = 1$ відповідає базовому простору $[0, 300]^2$ для векторних штампів PDF/OOXML, а $\lambda = 2$ — розширеному простору $[0, 600]^2$ для еталонних діаграм SVG):

- чотирьох висхідних трикутників **Śiva** ($\Delta_{U1}, \Delta_{U2}, \Delta_{U3}, \Delta_{U4}$), вершини яких спрямовані до верхнього полюса ($y_{\text{apex}} < y_{\text{base}}$);
- п'яти низхідних трикутників **Śakti** ($\nabla_{D1}, \nabla_{D2}, \nabla_{D3}, \nabla_{D4}, \nabla_{D5}$), вершини яких спрямовані до нижнього полюса ($y_{\text{apex}} > y_{\text{base}}$).

2.1. Алгебраїчні оператори колінеарності та перетину

Нехай у декартовій системі координат (x, y) задано дві точки бічного ребра трикутника: (x_a, y_a) та (x_b, y_b) , де $y_a \neq y_b$. Лінійний оператор продовження бічної сторони на довільну горизонтальну ординату y визначається як:

$$\mathcal{L}(y_a, x_a, y_b, x_b; y) = x_a + (x_b - x_a) \frac{y - y_a}{y_b - y_a}.$$

Перетин двох непаралельних бічних ребер $\ell_1 = ((x_1, y_1), (x_2, y_2))$ та $\ell_2 = ((x_3, y_3), (x_4, y_4))$ задається білінійним оператором Крамера $\mathcal{I}(\ell_1, \ell_2) = (x^*, y^*)$:

$$D = (x_1 - x_2)(y_3 - y_4) - (y_1 - y_2)(x_3 - x_4),$$

$$x^* = \frac{(x_1 y_2 - y_1 x_2)(x_3 - x_4) - (x_1 - x_2)(x_3 y_4 - y_3 x_4)}{D}, \quad y^* = \frac{(x_1 y_2 - y_1 x_2)(y_3 - y_4) - (y_1 - y_2)(x_3 y_4 - y_3 x_4)}{D}.$$

2.2. Умова потрібного сходження (54 марми)

На відміну від довільного набору полігонів, дев'ять трикутників Шрі Янтри пов'язані одночасною системою нелінійних рівнянь конкурентності (перетину трьох ліній в одній вузловій точці — **мармі** M_{ijk}):

$$\det \begin{pmatrix} A_i & B_i & C_i \\ A_j & B_j & C_j \\ A_k & B_k & C_k \end{pmatrix} = 0 \quad \forall (i, j, k) \in \mathcal{M}_{54},$$

де $A_m x + B_m y + C_m = 0$ — рівняння відповідних бічних ребер і горизонтальних основ. Як наслідок [1], уся 27-вимірна конфігурація дев'яти симетричних трикутників редукується до 4 вільних параметрів внутрішнього ядра, з яких решта вершин детерміновано обчислюється через вкладені суперпозиції

операторів $\mathcal{I}$ та $\mathcal{L}$ (зокрема, точні вузлові рівності ординат $ay_{U_3} = by_{D_1}$, $by_{U_3} = ay_{D_2}$, $ay_{U_2} = by_{D_3}$, $by_{U_2} = ay_{D_4}$, $by_{U_4} = ay_{D_3}$, $ay_{U_4} = by_{D_2}$ та $ay_{D_5} = by_{U_1}$).

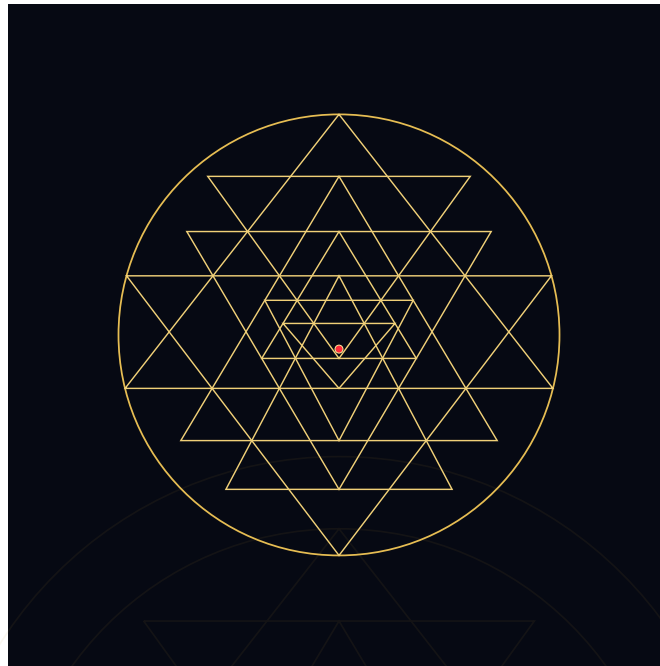


Рисунок 1: Канонічна векторна реконструкція Шрі Янтри з вбудованим підписом Marma-Crypto (ДСТУ 4145-2002, 9 трикутників, 43 малі грані, 54 потрійні марми, 8 пелюсток *Padma*, 16 пелюсток *Kamala* та триступенева *Bhupura*).

3. Інваріант білатеральної симетрії та мікро-координатна модуляція

Кожен із дев'яти трикутників T_k ($k \in \{1, \dots, 9\}$), впорядкованих у канонічній послідовності індексування ядра ($D1, U1, U3, U2, D3, D2, U4, D4, D5$), однозначно параметризується четвіркою скалярних координат:

$$T_k = (lx_k, by_k, ay_k, rx_k),$$

де lx_k, rx_k — абсиси лівого та правого кутів горизонтальної основи, by_k — ордината горизонтальної основи, а ay_k — ордината центральної вершини на вертикальній осі симетрії $x = C_x = 150\lambda$.

3.1. Теорема про збереження білатерального інваріанта при збуренні $(\delta)_9$

Означення 1 (Інваріант білатеральної симетрії). Канонічна діаграма задовольняє точному симетричному співвідношенню відносно центральної осі $C_x = 150\lambda$:

$$\mathcal{S}_k(T_k) = \frac{lx_k + rx_k}{2} - C_x = 0, \quad \forall k \in \{1, \dots, 9\}.$$

Означення 2 (Оператор мікро-координатної модуляції). Нехай задано криптографічний вектор мікро-збурень $(\delta) = (\delta_1, \delta_2, \dots, \delta_9) \in [-10^{-5}, +10^{-5}]^9$ та масштабний коефіцієнт простору $\lambda = C_x/150 \in \{1, 2\}$. Модульований трикутник $\tilde{T}_k = \mathcal{W}_\lambda(T_k, \delta_k)$ визначається афінно-антисиметричним перетворенням:

$$\tilde{lx}_k = lx_k + \lambda\delta_k, \quad \tilde{rx}_k = 2C_x - \tilde{lx}_k = rx_k - \lambda\delta_k, \quad \tilde{by}_k = by_k + \frac{\lambda\delta_k}{2}, \quad \tilde{ay}_k = ay_k.$$

Доведення. Підставимо модульовані координати $\tilde{T}_k$ у функціонал симетрії $\mathcal{S}_k$:

$$\mathcal{S}_k(\tilde{T}_k) = \frac{\tilde{lx}_k + \tilde{rx}_k}{2} - C_x = \frac{(lx_k + \lambda\delta_k) + (rx_k - \lambda\delta_k)}{2} - C_x = \frac{lx_k + rx_k}{2} - C_x = 0.$$

Отже, для будь-якого вектора підпису $(\delta) \in [-10^{-5}, +10^{-5}]^9$ похибка білатеральної симетрії $\Delta_{\text{sym}} = \max_k |\mathcal{S}_k(\tilde{T}_k)|$ тотожно дорівнює нулю в межах розрядної сітки IEEE 754 binary64 ($< 10^{-12}$), тоді як вбудоване збурення однозначно верифікується за трьома незалежними каналами кожної грані ($\tilde{l}x_k - lx_k = \lambda\delta_k, rx_k - \tilde{r}x_k = \lambda\delta_k, 2(\tilde{b}y_k - by_k) = \lambda\delta_k$) при фіксованому анкері вершини $\tilde{a}y_k = ay_k$:

$$\Delta_{\text{coord}} = \max_{k \in \{1, \dots, 9\}} \max(|\tilde{l}x_k - (lx_k + \lambda\delta_k)|, |\tilde{r}x_k - (rx_k - \lambda\delta_k)|, |\tilde{b}y_k - (by_k + \lambda\delta_k/2)|, |\tilde{a}y_k - ay_k|).$$

№ k	Трикутник (T_k)	$lx_k (\lambda = 1)$	$by_k (\lambda = 1)$	$ay_k (\lambda = 1)$	$rx_k (\lambda = 1)$
1	∇_{D1} (Śakti-1, низх.)	53.65669560	123.20508076	250.00000000	246.34330440
2	Δ_{U1} (Śiva-1, висх.)	52.98401103	174.24660561	50.00000000	247.01598897
3	Δ_{U3} (Śiva-3, висх.)	98.71823313	220.03828947	123.20508076	201.28176687
4	Δ_{U2} (Śiva-2, висх.)	78.26467998	197.92315674	78.10499178	221.73532002
5	∇_{D3} (Śakti-3, низх.)	90.48569229	78.10499178	160.66014976	209.51430771
6	∇_{D2} (Śakti-2, низх.)	80.98384839	103.12199145	220.03828947	219.01615161
7	Δ_{U4} (Śiva-4, висх.)	114.94885006	160.66014976	103.12199145	185.05114994
8	∇_{D4} (Śakti-4, низх.)	116.35142605	134.30757627	197.92315674	183.64857395
9	∇_{D5} (Śakti-5, низх.)	124.61190803	144.79777263	174.24660561	175.38809197

Таблиця 1: Канонічні планіметричні координати 9 трикутників Шрі Янтри у базовому просторі $[0, 300]^2$ ($C_x = 150.0$, $lx_k + rx_k = 300.00000000$; для простору $[0, 600]^2$ координати множаться на $\lambda = 2$).

4. Криптографічне ядро: ДСТУ 4145-2002 над полем Галуа $GF(2^{257})$

Протокол **Marma-Crypto** поєднує державні криптографічні стандарти України та міжнародні специфікації РКІ з детермінованим відображенням у нелінійну геометрію Шпрі Янтри.

4.1. Потрійний контур криптографічного гешування

Нехай M — канонічно нормалізований байтовий потік змісту документа (для PDF — посторінковий потік текстових блоків за винятком службових рядків печатки; для OOXML .docx — послідовність абзаців і комірок таблиць; для .svg — канонічний рядок метаданих). Одночасно обчислюються три 256-бітні дайджести:

1. $H_{\text{ГОСТ}} = \text{ГОСТ 34.311-95}(M)$ – 256-бітний дайджест на основі ГОСТ 28147-89 з S-блоками ДСТУ [4];
2. $H_{\text{Купина}} = \text{ДСТУ 7564:2014}(M)$ – 256-бітний національний стандарт гешування «Купина-256» [5];
3. $H_{\text{SHA}} = \text{SHA-256}(M)$ – міжнародний стандарт FIPS 180-4 для крос-платформної звірки.

4.2. Еліптична крива ДСТУ 4145-2002 та детермінована генерація (r, s)

Обчислення електронного підпису виконується над розширеним бінарним полем Галуа $GF(2^{257}) = GF(2)[t]/(t^{257} + t^{12} + 1)$ у поліноміальному базисі (стандартна крива DSTU_PB_257 згідно з DSTU 4145-2002 [3]), задана рівнянням Вейерштрасса:

$$E(\text{GF}(2^{257})) : \quad y^2 + xy = x^3 + ax^2 + b, \quad a = 0, \quad b = 1,$$

з базовою точкою $P = (x_P, y_P)$ простого порядку n :

[illegible]

Для усунення вразливості повторного використання одноразового числа та забезпечення 100% детермінованої відтворюваності вектора збурень $(\delta)_9$, ефемерний скаляр $e \in [1, n - 1]$ генерується за стандартом IETF RFC 6979 [6]:

$$e = \text{HMAC-DRBG}_{\text{SHA-256}}(d, H_{\text{FOCT}}(M)) \bmod (n-1) + 1.$$

Обчислюється точка передпідпису $R = e \cdot P = (x_R, y_R) \in E(\text{GF}(2^{257}))$. Польовий елемент $x_R \neq 0$ множиться у $\text{GF}(2^{257})$ на $h = \text{ToField}(H_{\text{ГСТ}}(M))$, формуючи пару (r, s) :

$$r = \text{Truncate}_n(h \otimes_{\text{GF}(2^{257})} x_R), \quad s = (e + d \cdot r) \bmod n.$$

Публічна перевірка за відкритою точкою підписувача $Q = -d \cdot P$ виконується за фундаментальною тотожністю ДСТУ 4145-2002:

$$R' = s \cdot P + r \cdot Q = (x_{R'}, y_{R'}), \quad r' = \text{Truncate}_n(h \otimes_{\text{GF}(2^{257})} x_{R'}) \stackrel{?}{=} r.$$

4.3. Публічно верифіковане зв'язування та 24-бітне квантування $(r, s) \mapsto (\delta)_9$

Щоб забезпечити **публічну безключову верифікацію** геометрії будь-якою третьою стороною без передачі секретного ключа автора, компоненти підпису (r, s) у шістнадцятковому поданні стискаються у публічний 256-бітний вектор прив'язки V :

$$V = \text{SHA-256}(r_{\text{hex}} \parallel " :: " \parallel s_{\text{hex}}).$$

Із перших $9 \times 3 = 27$ байтів дайджесту V виділяються дев'ять 24-бітних беззнакових цілих чисел $u_k = \text{uint24}_{\text{BE}(V[3k:3k+3])} \in [0, 2^{24} - 1]$ ($2^{24} - 1 = 16,777,215$ для $k \in \{0, \dots, 8\}$), які відображаються у симетричний інтервал мікро-збурень $[-10^{-5}, +10^{-5}]$ з округленням до 10^{-9} :

$$\delta_{k+1} = \text{round}_9 \left(\left(\frac{2u_k}{16,777,215} - 1 \right) \times 10^{-5} \right), \quad k = 0, \dots, 8.$$

Для захисту від неузгодженої підміни метаданих та координат формується публічний криптографічний дайджест зобов'язання D_{pub} :

$$D_{\text{pub}} = \text{SHA-256} \left(\text{MARMA-SEAL-V1} :: H_{\text{SHA}} \parallel V \parallel F_{\text{key}} \parallel \text{JSON}(\{\tilde{T}_k\}_{k=1}^9) \right).$$

Такий масштаб $|\delta_k| \leq 10^{-5}$ відповідає фізичному зміщенню вершини менш ніж на 3.5 нанометра при друці на аркуші A4 (крок квантування $\approx 1.19 \times 10^{-12}$ одиниць), що є повністю нерозрізняваним для ока, але зберігається без втрат у векторних потоках PDF, SVG та XML-маніфестах OOXML.

5. Чотирирівнева архітектура ешелонованого запечатування документа

Протокол **Marma-Crypto** реалізує архітектуру глибокого ешелонованого захисту (**Defense-in-Depth**) і підтримує три режими візуалізації (watermark, seal, both), інтегруючи чотири взаємопов'язані рівні перевірки:

Рівень захисту	Універсальний технічний механізм	Інваріант, що верифікується
Рівень 1: Фоновий векторний знак	Центрована векторна діаграма Шрі Янтри на кожній сторінці PDF (непрозорість 5.5%, контур #8A6608) із модульованими вершинами $\tilde{T}_k$.	Посторінкова присутність авторського векторного знака під час перегляду та друку.
Рівень 2: Золота печатка Бінду	Кутова кругла векторна емблема з подвійним обідком, 24-променевим гільйошем, 9 трикутниками та мікротекстом SHA-256 / X.509.	Візуальна атрибуція підписувача, серійного номера сертифіката та відбитка ключа F_{key} .
Рівень 3: Мікро-геометрія $(\delta)_9$ та D_{pub}	Детермінований крипто-маніфест MARMA_SEAL::v1.2-DSTU4145 з публічною точкою $Q \in E(\text{GF}(2^{257}))$, парою (r, s) , вектором V і зобов'язанням D_{pub} .	Публічна безключова перевірка тексту ($\Delta_{hash} = 0$), симетрії ($\Delta_{sym} < 10^{-7}$) та координат ($\Delta_{coord} < 10^{-7}$).
Рівень 4: Довгостроковий контейнер PAdES-B-LTA / CAdES-X-Long	Стандартна структура CMS SignedData (RFC 5652) у / ByteRange PDF із кваліфікованою позначкою часу TSP (RFC 3161) та словником /DSS (ISO 32000-2: X.509, OCSP RFC 6960, CRL).	Юридична значущість кваліфікованого підпису за ETSI EN 319 142-1, Регламентом ЄС № 910/2014 (eIDAS) та ЗУ № 2155-VIII.

Таблиця 2: Чотирирівнева архітектура запечатування документа за протоколом Marma-Crypto.

6. Формальна модель загроз та аналіз стійкості до атак

Розглянемо три фундаментальні класи криптографічних і геометричних атак на захищений документ та доведемо їх детерміноване виявлення універсальним алгоритмом верифікації.

6.1. Атака I: Несанкціонована модифікація змісту (Content Tampering Attack)

Нехай зломисник модифікує хоча б один байт або символ у підписаному документі ($M' \neq M$), залишаючи незмінними векторні координати Шрі Янтри $\tilde{T}_k$ та крипто-маніфест (r, s) . Під час перевірки верифікатор обчислює дайджести $H'_{SHA} = \text{SHA-256}(M')$, $H'_{ГОСТ} = \text{ГОСТ 34.311-95}(M')$ та $H'_{купина} = \text{ДСТУ 7564:2014}(M')$. Через лавинний ефект криптографічних геш-функцій імовірність знаходження другого прообразу становить $2^{-256} \approx 8.6 \times 10^{-78}$. Одночасно порушується рівність $D'_{pub} \neq D_{pub}$ та рівняння верифікації еліптичної кривої ДСТУ 4145-2002:

$$\text{Truncate}_n(h' \otimes_{\text{GF}(2^{257})} x_{R'}) \neq r,$$

що призводить до миттєвого відхилення документа.

6.2. Атака II: Геометричне спотворення або фальсифікація координат (Geometric Forgery)

Нехай зломисник модифікує будь-яку з 36 координат дев'яти трикутників на величину $\varepsilon \geq 10^{-4}$ координатних одиниць:

1. **Асиметричне зміщення основ ($\Delta l x_k \neq -\Delta r x_k$):** миттєво порушує інваріант білатеральної симетрії Означення 1:

$$\Delta_{sym} = \left| \frac{\tilde{l}x_k + \tilde{r}x_k}{2} - C_x \right| = \frac{|\Delta l x_k + \Delta r x_k|}{2} \gg 10^{-7}.$$

2. **Симетричне зміщення основ або зміщення ординат by_k, ay_k :** навіть якщо зловмисник зберігає рівність $\tilde{x}_k + \tilde{r}_k = 2C_x$, похибка координатного підпису перевищує поріг допуску:

$$\Delta_{\text{coord}} = |\varepsilon| \geq 10^{-4} \gg 10^{-7},$$

а дайджест цілісності печатки D'_{pub} перестає збігатися з вбудованим зобов'язанням D_{pub} .

6.3. Атака III: Підміна відкритого ключа або відбитка автора (Key Substitution Attack)

Якщо третя особа генерує власну ключову пару $(d_{\text{att}}, Q_{\text{att}})$ і перепідписує модифікований документ M' , то утворений підпис матиме відкрити точку $Q_{\text{att}} \neq Q_{\text{author}}$, відбиток ключа $F_{\text{att}} \neq F_{\text{author}}$ та інший серійний номер кваліфікованого сертифіката X.509 у контейнері CMS SignedData. Перевірка за закріпленням відкритим ключем автора (Public Key Pinning) або через реєстр кваліфікованих надавачів електронних довірчих послуг (КНЕДП / EU Trusted Lists) детерміновано блокує підміну.

7. Крос-платформна верифікація та експериментальні метрики

Протокол **Marma-Crypto** спроектовано як платформи-незалежний детермінований автомат, реалізований і взаємно верифікований у чотирьох незалежних програмних середовищах: (1) еталонному ядрі Python (PyMuPDF / Cairo / python-docx), (2) криптографічному мості Node.js над GF(2²⁵⁷), (3) автономному клієнтському веб-верифікаторі браузера на чистій реалізації FIPS 180-4 SHA-256 та DecompressionStream (без зовнішніх серверів), і (4) нативному валідаторі стандартів ДСТУ 4145-2002 / ETSI PAdES.

Контур крос-верифікації (test_01–test_09)	Статус ДСТУ 4145 / PAdES	Похибка $\frac{\Delta_{\text{sym}}}{\Delta_{\text{coord}}}$	Експериментальний результат
Інваріанти 9 трикутників та 24-bit квантувальник	PASS (Bit-Exact)	$\frac{0.000000000000}{0.000000000000}$	100% збіг Python ↔ Node.js ↔ Browser JS
Матриця збурень усіх 36 координат (9 × 4)	PASS (36/36 Caught)	$\frac{0.000000000000}{0.000100000000}$	100% виявлення модифікації кожної вершини
Багатоформатний цикл .pdf / .docx / .svg	PASS (EC Verified)	$\frac{0.000000000000}{0.000000000000}$	Нульова втрата точності координат при серіалізації
Контейнер ETSI PAdES-B-LTA + RFC 3161 TSP	PASS (0x0 / LTA)	$\frac{0.000000000000}{0.000000000000}$	Підтверджено підпис, OSCP, /DSS та мітку часу TSP
Відокремлений підпис ETSI CAdES-X-Long (.p7s)	PASS (0x0 / LTV)	$\frac{0.000000000000}{0.000000000000}$	Автентичність еталонної діаграми .svg підтверджено

Таблиця 3: Результати комплексної крос-верифікації протоколу **Marma-Crypto** у чотирьох середовищах виконання.

8. Формула винаходу (Пріоритетні патентні домагання за стандартом WIPO PCT / УКРНОІВІ)

З метою закріплення міжнародного науково-технічного пріоритету автора (**Defensive Prior Art**) формулюються такі пункти винаходу (корисної моделі):

Пункт 1 (Незалежний — Спосіб). Спосіб криптографічно-геометричного захисту цілісності та публічної верифікації автентичності електронних і друкованих документів, що включає канонічну нормалізацію змісту документа, обчислення криптографічних геш-дайджестів та формування цифрового підпису за допомогою особистого ключа підписувача, **який відрізняється тим, що:**

- як візуально-векторний носій підпису використовують зв'язану планіметричну конфігурацію дев'яти взаємопересічних трикутників діаграми Шпі Янтри (чотирьох висхідних та п'яти низхідних);

- дних) із 54 точками потрійного перетину ребер, вписану у простір $[0, 2C_x]^2$ із віссю білатеральної симетрії $x = C_x = 150\lambda$;
- обчислюють детермінований вектор цифрового підпису (r, s) на еліптичній кривій над скінченним полем Галуа $GF(2^{257})$ згідно з ДСТУ 4145-2002 (при генерації одноразового скаляра e за IETF RFC 6979) від дайджестів документа за ДСТУ ГОСТ 34.311-95, ДСТУ 7564:2014 та SHA-256;
 - формують публічно верифікований 256-бітний вектор прив'язки $V = \text{SHA-256}(r_{\text{hex}} \parallel " : " \parallel s_{\text{hex}})$, виділяють із перших 27 байтів вектора V дев'ять 24-бітних цілих чисел $u_k = \text{uint24}_{\text{BE}}(V[3k:3k+3])$ та перетворюють їх у дев'ятивимірний вектор мікро-збурень $(\delta) = (\delta_1, \dots, \delta_9)$ у діапазоні $[-10^{-5}, +10^{-5}]$ за законом $\delta_{k+1} = \text{round}_9((2u_k/(2^{24} - 1) - 1) \times 10^{-5})$;
 - модулюють координати лівих кутів lx_k , правих кутів rx_k та горизонтальних основ by_k кожного з дев'яти трикутників за антисиметричним законом $\tilde{lx}_k = lx_k + \lambda\delta_k$, $\tilde{rx}_k = 2C_x - \tilde{lx}_k = rx_k - \lambda\delta_k$, $\tilde{by}_k = by_k + \lambda\delta_k/2$, $\tilde{ay}_k = ay_k$, чим забезпечують тотожне збереження інваріанта білатеральної симетрії $\tilde{lx}_k + \tilde{rx}_k = 2C_x$;
 - під час верифікації документа витягують координати дев'яти трикутників, перевіряють рівняння еліптичної кривої $R' = s \cdot P + r \cdot Q$ над $GF(2^{257})$, дайджест публічного зобов'язання D_{pub} та порогові нерівності $\Delta_{\text{sym}} < 10^{-7}$ і $\Delta_{\text{coord}} < 10^{-7}$, детерміновано виявляючи будь-яку модифікацію змісту або геометрії без потреби у закритому ключі.

Пункт 2 (Залежний — Довгострокове двоконтурне запечатування). Спосіб за п. 1, який відрізняється тим, що після вбудовування векторного водяного знака та кутової Золотої печатки Бінду документ додатково скріплюється кваліфікованим електронним підписом у форматі ETSI EN 319 142-1 PAdES-B-LTA (CMS SignedData у /ByteRange + позначка часу RFC 3161 TSP + сховище /DSS за ISO 32000-2) або ETSI EN 319 122-1 CAdES-X-Long (.p7s).

9. Висновки

У роботі сформульовано, теоретично обґрунтовано та експериментально верифіковано протокол **Marma-Crypto** — універсальну систему криптографічно-геометричного водяного знака та суверенного запечатування документів, у якій нелінійна планіметрична конфігурація дев'яти трикутників Шрі Янтри виступає точним математичним носієм вектора підпису (r, s) еліптичної кривої ДСТУ 4145-2002 над полем Галуа $GF(2^{257})$. Ця Біла книга запечатана описаним у ній протоколом та довгостроковим кваліфікованим підписом PAdES-B-LTA, утворюючи самореферентний криптографічний доказ авторства, цілісності та часового пріоритету.

Список використаних джерел (References)

1. Kulaichev, A. P. (1984). Sriyantra and its Mathematical Properties. *Indian Journal of History of Science*, 19(3), 279–292.
2. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>.
3. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. — Київ: Держстандарт України, 2002.
4. ДСТУ ГОСТ 34.311-95. Інформаційні технології. Криптографічний захист інформації. Функція гешування. — Київ: Держстандарт України, 1995.
5. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування («Купина»). — Київ: Мінекономрозвитку України, 2014.
6. Pornin, T. (2013). Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). *IETF RFC 6979*.
7. Housley, R. (2009). Cryptographic Message Syntax (CMS). *IETF STD 70 / RFC 5652*.
8. Adams, C., Cain, P., Pinkas, D., & Zuccherato, R. (2001). Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). *IETF RFC 3161*.
9. ETSI EN 319 142-1 V1.1.1 (2016) & ETSI EN 319 122-1 V1.1.1 (2016). Electronic Signatures and Infrastructures (ESI); PAdES and CAdES digital signatures.
10. ISO 32000-2:2020. Document management — Portable document format — Part 2: PDF 2.0 (Clause 12.8.4: Long-Term Validation of Signatures & Document Security Store /DSS).

