УДК 004.056.523:004.93’1
DOI: 10.31673/2409-7292.2024.020007

Кашапов А. А., Нємкова О. А.

РОЗРОБЛЕННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ ДИНАМІЧНИХ ШАБЛОНІВ АВТЕНТИФІКАЦІЇ

Застосування електронного цифрового підпису для автентифікації електронних пристроїв відзначається важливістю і актуальністю в контексті сучасних цифрових технологій та кібербезпеки. Кожен електронний пристрій може мати свій власний унікальний цифровий підпис, який створюється за допомогою криптографічних алгоритмів. Цей підпис вбудовується в електронну інформацію та дозволяє перевіряти, чи не були дані під час передачі або зберігання підроблені чи змінені. Робота присвячена розробці електронного цифрового підпису на основі динамічних шаблонів автентифікації. У роботі висвітлено основні принципи функціонування електронного цифрового підпису та переваги використання динамічних шаблонів для забезпечення безпеки автентифікації електронних пристроїв. Досліджено основні методи захисту від компрометації електронного цифрового підпису і реалізовано схему одноразового електронного цифрового підпису на основі динамічних шаблонів автентифікації із застосуванням пуасонівських імпульсних послідовностей. Підхід, що базується на унікальних характеристиках електронних пристроїв через генерацію шаблонів автентифікації, виявив великий потенціал для підвищення рівня безпеки та надійності для процесу автентифікації електронних пристроїв. Ротація ключів, одноразові електронні цифрові підписи та динамічні шаблони автентифікації на основі унікальних характеристик електронних пристроїв є ключовими методами, які забезпечують стійкість електронного цифрового підпису і уможливлюють безпечне застосування ЕЦП в контексті автентифікації електронних пристроїв. Результати роботи можуть мати важливе значення для розвитку безпеки електронних систем та засобів автентифікації в контексті застосування електронних цифрових підписів.

Ключові слова: кібербезпека, електронний цифровий підпис, динамічні шаблони автентифікації, автентифікація електронних пристроїв, одноразові електронні цифрові підписи.

Вступ

Застосування електронного цифрового підпису для автентифікації електронних пристроїв відзначається важливістю і актуальністю в контексті сучасних цифрових технологій та кібербезпеки. ЕЦП виступає ключовим засобом забезпечення автентичності, конфіденційності і цілісності інформації в електронних системах та мережах [1].

Об’єктом дослідження є електронний цифровий підпис. Предметом дослідження є застосування електронного цифрового підпису для автентифікації електронних пристроїв. Наукова новизна роботи полягає в розроблені схеми одноразового електронного цифрового підпису на основі пуасонівських імпульсних послідовностей. Практичним значенням отриманих результатів є варіант вирішення досліджених проблем безпеки при застосуванні електронного цифрового підпису для автентифікації електронних пристроїв.

Робота висвітлює такі науково значущі аспекти: комплексний погляд на ЕЦП в контексті автентифікації, дослідження методів захисту ЕЦП, сучасні тенденції в автентифікації електронних пристроїв за їх унікальними характеристиками і практичний та науковий внесок до сфери застосування ЕЦП як засобу автентифікації електронних пристроїв на основі динамічних шаблонів автентифікації із застосуванням пуасонівських імпульсних послідовностей.

Формулювання проблеми

Електронний цифровий підпис є важливим засобом для автентифікації електронних пристроїв і забезпечення їхньої безпеки в сучасному цифровому світі. Одним із основних застосувань ЕЦП є захист від фальсифікації та забезпечення автентичності пристроїв [1]. Кожен електронний пристрій може мати свій власний унікальний цифровий підпис, який створюється за допомогою криптографічних алгоритмів. Цей підпис вбудовується в електронну інформацію та дозволяє перевіряти, чи не були дані під час передачі або зберігання підроблені чи змінені. Це забезпечує високий рівень довіри до електронних пристроїв та даних, що обмінюються між ними.

При роботі з ЕЦП виникають проблеми стосовно безпеки. Взаємодія з приватними ключами ЕЦП потребує високого рівня безпеки, оскільки їх втрата може призвести до

компрометації даних. Іншою важливою проблемою є автентичність публічних ключів, використовуваних для перевірки ЕЦП – вони повинні бути надійно пов'язані з конкретними пристроями та їх власниками.

Підхід автентифікації електронних пристроїв за їх унікальними характеристиками шляхом генерації унікальних шаблонів автентифікації дозволяє сформувати висновки про ідентичність пристрою на основі його фізичних, технічних та програмних особливостей, що включають в себе біометричні дані, апаратне забезпечення та структурні характеристики [2]. Ця робота висвітлює актуальність і значущість цього підходу, а також ставить завдання дослідження методів генерації шаблонів автентифікації, що сприяють підвищенню рівня безпеки та надійності процесу автентифікації електронних пристроїв.

Аналіз літератури

Застосування ЕЦП для автентифікації електронних пристроїв потребує вдосконалення та вивчення різних аспектів безпеки та інфраструктури ключів. Розробники та організації повинні враховувати ці виклики, планувати відповідні заходи безпеки та вдосконалювати методи захисту для забезпечення надійної автентифікації пристроїв з використанням електронних цифрових підписів.

До основних проблем при роботі з ЕЦП можна навести такі аспекти [3]:

Автентичність ключів: Важливо переконатися, що публічний ключ, що використовується для перевірки ЕЦП, належить саме тому пристрою, що ідентифікується. Існує ризик, що ключ може бути підроблений або скомпрометований, особливо при користуванні відкритими каналами передачі інформації або в ненадійних середовищах.

Відкритість ключів: Застосування публічних ключів пристроїв, які є відкритими і доступними для інших, може створити ризики, особливо якщо публічні ключі можуть бути використані для визначення, який пристрій власнику належить.

Атаки на ключі: Приватні ключі можуть бути предметом атак і витоків даних (англ. Data Breach). Зловмисники можуть намагатися отримати доступ до цих ключів для підробки підписів чи компрометації інформації.

Легітимність користувача: ЕЦП не завжди гарантує, що сам користувач є легітимним. Якщо ключі не безпечно зберігаються або доступні недостатньо захищеною автентифікацією, зловмисники можуть використовувати ЕЦП навіть без дозволу власника.

Квантові обчислення: З розвитком квантових обчислень існує загроза, що квантові комп’ютери наражатимуть на небезпеку сучасні криптографічні алгоритми, використані для роботи з ЕЦП.

Сучасні дослідження в галузі застосування електронного цифрового підпису для автентифікації електронних пристроїв визначаються рядом ключових напрямків та інновацій, спрямованих на підвищення безпеки та надійності цього процесу [1, 4, 5]. Загальна мета цих досліджень полягає в розробці та вдосконаленні методів, які допомагають забезпечити високий рівень безпеки та надійності автентифікації електронних пристроїв в умовах постійно зростаючих викликів кібербезпеки.

Автентифікація за унікальними характеристиками дозволяє підвищити безпеку та ідентифікацію пристрою, а також зменшити ризик несанкціонованого доступу до конфіденційних ресурсів. Автентифікація відбувається в процесі ідентифікації пристрою на основі унікальних атрибутів або характеристик, які дозволяють відрізнити певний пристрій від інших (рис. 1).

Одним із незалежних від типу електронного пристрою методом є метод формування шаблонів автентифікації з використанням електронних шумів, що є інноваційним підходом до забезпечення безпеки та процесу автентифікації, який опрацьовує електронні шуми, що виникають у електронних пристроях, як унікальний шаблон автентифікації для певного пристрою [7]. Кожен електронний пристрій генерує ці електронні шуми під час нормальної роботи через випадкові процеси в електронних компонентах. Оскільки ці шуми є унікальними

і непередбачуваними, вони можуть формувати неповторні ідентифікаційні шаблони для кожного пристрою.

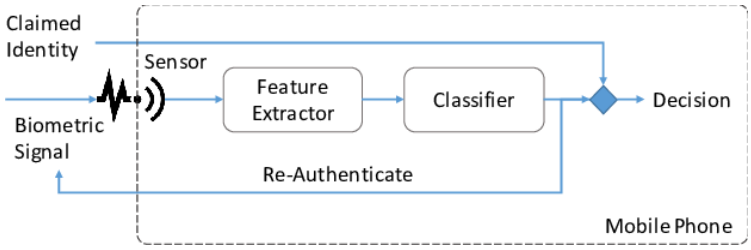

Рис. 1. Загальна схема процесу автентифікації з використанням шаблонів автентифікації [6]

Іншим методом, що використовує унікальність фізичних властивостей електронних пристроїв є метод формування шаблонів автентифікації з використанням генератора випадкових чисел, що залежить від зовнішньої частоти [2]. В цьому методі використовуються фізичні процеси для генерації випадкових даних, які служать основою для створення унікальних автентифікаційних шаблонів для пристроїв.

Мета та завдання дослідження

Мета дослідження полягає у розроблені схеми електронного цифрового підпису на основі динамічних методів автентифікації.

Для досягнення цієї мети необхідно виконати такі завдання:

1. Дослідити можливості застосування електронного цифрового підпису для задачі автентифікації електронних пристроїв;
2. Провести аналіз методів захисту електронних цифрових підписів;
3. Провести аналіз методів формування динамічних шаблонів автентифікації для електронних пристроїв;
4. Розробити схему електронного цифрового підпису на основі динамічних шаблонів автентифікації;
5. Опрацювати отримані дані та сформувати висновки до результатів виконання роботи.

Застосування ротації ключів та одноразових електронних цифрових підписів

Ротація ключів для електронного цифрового підпису – це процес періодичної зміни криптографічних ключів, які використовуються для створення електронних цифрових підписів і їх перевірки. Цей процес важливий для підвищення безпеки і захисту від потенційних атак, оскільки ключі мають обмежений строк дії, і їх часта зміна зменшує ризик компрометації [8].

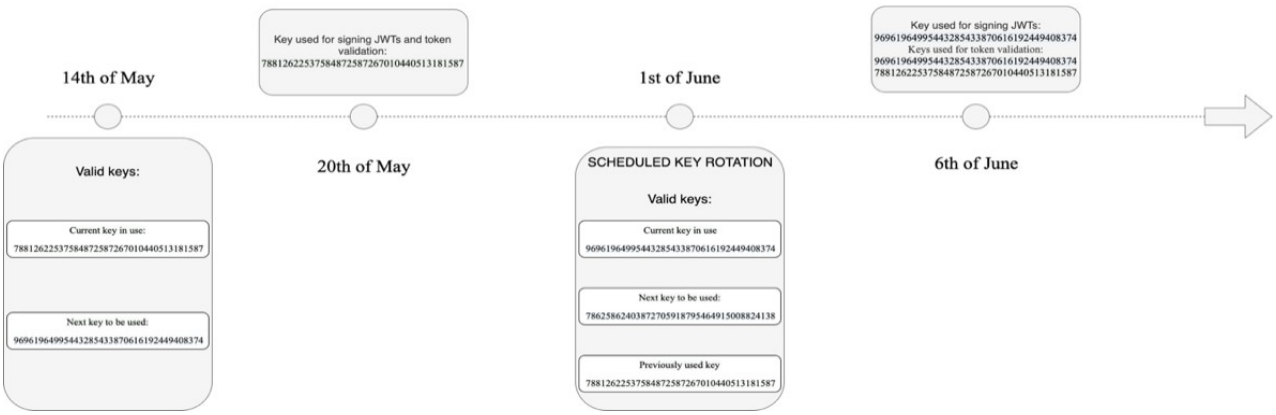

Рис. 2. Схема прикладу автоматизованого розкладу ротації ключів [9]

Одноразовий електронний цифровий підпис може бути розглянутий як частковий випадок ротації ключів у системі криптографічного захисту [10]. У цьому контексті використовується унікальний ключ для кожного підпису, і він використовується лише один раз, після чого замінюється новим ключем. Такий підхід має свою вагому перевагу в унікальності ключа для кожного підпису, що робить його особливо стійким до атак та підвищує рівень безпеки. Кожен новий підпис використовує новий ключ, а отже, навіть якщо один ключ стане вразливим, це не вплине на інші підписи. Такий метод також може слугувати додатковим заходом безпеки в системах, де ключі можуть стикатися з ризиком викриття або компрометації.

Генерація одноразового ЕЦП вимагає використання спеціальних алгоритмів, які забезпечують унікальність формування підпису. Основною властивістю досліджених алгоритмів створення одноразових ЕЦП є застосування хеш-функцій [11]. Дані, які потрібно підписати, піддаються хешуванню, і результат обчислення стає одноразовим підписом. При кожному новому підписі генерується новий хеш, що робить підпис унікальним.

Електронні цифрові підписи на основі хеш-функцій класифікується за одноразовістю сформованого підпису і внутрішньою структурою [11]:

одноразові (Лампорта, Вінтерніца);

багаторазові з використанням дерев Мерклі;

багаторазові з поступовим зниженням стійкості (HORS, HORST, FORS, PORS);

багаторазові з використанням гіпердерев (SPHINCS, SPHINCS+, Gravity-SPHINCS, XMMSMT).

Підпис Лампорта, тип криптографічної схеми одноразового підпису, був представлений Леслі Лампортом у 1979 році як проста і безпечна альтернатива традиційним цифровим підписам. Він використовується для одноразових підписів і забезпечує унікальний підхід до захисту цифрових комунікацій [12].

Фундаментальна ідея підписів Лампорта полягає у використанні криптографічних хеш-функцій для підписання повідомлень. У схемі підпису Лампорта процес генерації ключа є критично важливим етапом. Генеруються два масиви попередніх репрезентацій криптографічного хешу, один для 0-бітів, а інший для 1-бітів у двійковому представленні приватного ключа. Ці масиви формують приватний ключ підпису. Відповідний відкритий ключ отримується шляхом хешування попередніх репрезентацій в масивах.

Формування шаблонів автентифікації з використанням генератора пуасонівських імпульсних послідовностей

Універсальною схемою формування динамічних шаблонів автентифікації є побудова автентифікаційних ознак на основі генераторів пуасонівських імпульсних послідовностей. Протягом тривалого часу генератори випадкових або псевдовипадкових імпульсних послідовностей використовувалися для вирішення різноманітних завдань у науці та техніці [12]. Серед ключових генераторів є генератор пуасонівських імпульсних послідовностей (ГПІП), який широко використовується в різних технічних галузях для моделювання процесів, що характеризуються випадковими часовими та просторовими атрибутами. Ці генератори знаходять застосування в таких галузях, як соціологічні та наукові дослідження. Крім того, вони виявляються ефективними у вирішенні проблем кібербезпеки [2].

В аналізованому дослідженні, використовуючи отримані дані про генератори пуасонівських імпульсних послідовностей та досягнення в теорії контрольних кодів, було програмно згенеровано набір пуасонівських імпульсних послідовностей [2]. Використовуючи ці послідовності, було сформовано модель динамічних шаблонів автентифікації для зразків пристроїв і програмно виконано процедури автентифікації. Оцінка результати автентифікації складалася з обчислення пар відстаней Хемінга як між шаблонами автентифікації одного пристрою (внутрішні відстані Хемінга), так і між шаблонами автентифікації різних пристроїв (зовнішні відстані Хемінга), а потім порівняння цих відстаней (рис. 3).

Для генерації динамічних шаблонів автентифікації було використано генератор пуасонівських імпульсних послідовностей, структурна схема якого наведена нижче (рис. 4).

Наведений генератор складається з модифікованого адитивного генератора Фібоначчі (МАФГ), що містить регістри Rg1-Rg5, суматори Ad1-Ad3, логічну схему LS, що відповідає за формування допоміжної змінної, що відповідає значенню псевдовипадкового біта, а також схему порівняння CS та логічний елемент & (логічне І). Всі структурні елементи МАФГ, крім логічної схеми LS, працюють в двійково-десятковому коді (англ. BCD, Binary-Coded Decimal).

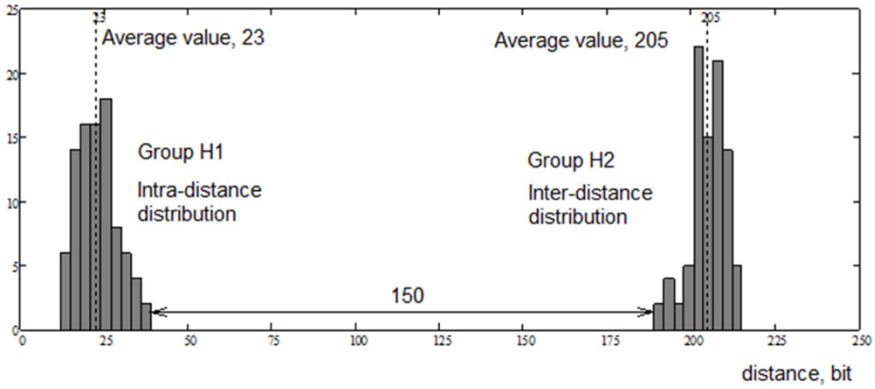

Рис. 3. Гістограма розподілу відстаней Хемінга для електронного пристрою і сформованих шаблонів автентифікації того ж самого пристрою (внутрішні відстані групи H1) та іншого пристрою (зовнішні відстані групи H2) [2]

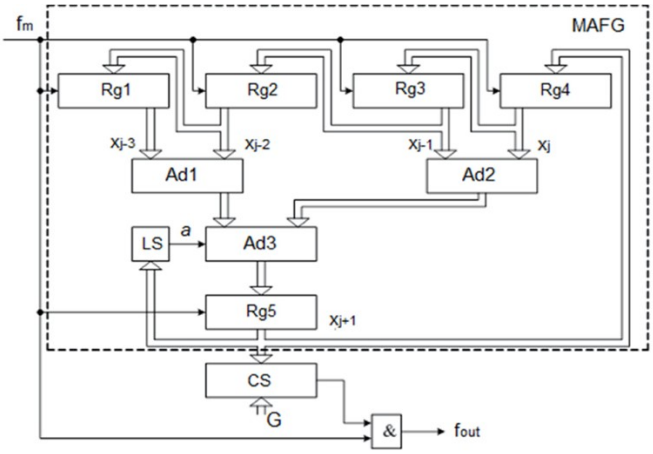

Рис. 4. Структурна схема генератора пуасонівських імпульсних послідовностей [2]

Послідовність псевдовипадкових чисел формується на виході модифікованого адитивного генератора Фібоначчі, тобто на виході регістру Rg5, згідно наведеного виразу:

$$x_{j+1} = (x_j + x_{j-1} + x_{j-2} + x_{j-3} + a) \bmod m,$$

де x_{j+1} – псевдовипадкове число, що формує послідовність псевдовипадкових чисел;

x_j, x_{j-1}, x_{j-2}, x_{j-3} – числа, збережені в регістрах Rg4, Rg3, Rg2, Rg1 відповідно;

$m = 10^q$ – модуль псевдовипадкового числа, значення q дорівнює кількості десяткових розрядів в структурних елементах схеми;

a – значення псевдовипадкового біта.

Псевдовипадковий біт a, що застосовується при формуванні послідовності псевдовипадкових чисел, обчислюється для кожного числа з послідовності за формулою:

$$a = \left(a_0^0 \oplus a_0^1 \oplus a_0^2 \oplus a_0^3\right) \oplus \cdots \oplus \left(a_{q-1}^0 \oplus a_{q-1}^1 \oplus a_{q-1}^2 \oplus a_{q-1}^3\right),$$

де a_i^j, $i = 0, 1, \ldots, q - 1$, $j = 0, 1, 2, 3$ – значення бітів у двійково-десятковому коді числа в регістрі Rg5.

Кількість членів в наведеній формулі залежить від значення параметра q і обирається з проміжку $0, 1, \ldots, 4 \cdot q$. Детальну інформацію про параметри вихідного сигналу і внутрішні параметри генератора та їх взаємозв'язок, і методи оцінювання статистичних характеристик вихідного сигналу наведено в дослідженні [2].

Використання генератора пуасонівських імпульсних послідовностей, налаштованого на q = 6 і G = 10 000, дає бітову послідовність A, в якій переважають 0-біти, з в середньому десятьма 1-бітами на тисячу бітів. Позиції окремих бітів у кожному 1000-бітному фрагменті не збігаються. Для моделювання шаблонів реального часу того ж пристрою рекомендується обрати контрольний код G = 10 000, що призводить до середньої відстані Хемінга 20 між парами таких фрагментів. В якості альтернативи, при q = 6 і значенні контрольного коду G = 100 000, згенерована послідовність B має в середньому сто 1-бітів на тисячу бітів, що призводить до середньої відстані 200 між двома 1000-бітними фрагментами послідовності B.

Комбінація з використанням прямої суми фрагментів послідовностей A і B використовується для формування шаблонів автентифікації. Для кожного електронного пристрою спочатку створюється еталонний шаблон, з яким порівнюватимуться динамічні шаблони. Для формування еталонного бітового шаблону для електронного пристрою N, необхідно об'єднати один 1000-бітний фрагмент послідовності B, з одним 1000-бітовим фрагментом послідовності *A*.

Динамічні шаблони автентифікації для електронного пристрою *N* формуються згідно наведеного виразу:

$$BT_{N_M} = B_N \oplus A_M,$$

де BT_{N_M} – M-й шаблон автентифікації пристрою *N*;

B_N – фрагмент бітової послідовності *B*, що використовується для формування шаблонів автентифікації для електронного пристрою *N*;

A_M – M-й фрагмент бітової послідовності *A*.

Програмна модель одноразового електронного цифрового підпису на основі пуасонівських імпульсних послідовностей

Процес створення і застосування одноразового електронного цифрового підпису на основі пуасонівських імпульсних послідовностей для автентифікації електронних пристроїв може бути поділений на такі ключові етапи:

1. Ініціалізація параметрів: Спочатку визначаються параметри алгоритму генерації пуасонівської імпульсної послідовності – значення коду управління і кількості відрізків бітових послідовностей.

2. Генерація пуасонівських імпульсних послідовностей: За допомогою дослідженого методу генерується дві пуасонівські імпульсні послідовності. Ці послідовності будуть використовуватися як основа для створення динамічних шаблонів автентифікації для електронного цифрового підпису.

3. Формування шаблонів автентифікації: Згенеровані пуасонівські імпульсні послідовності застосовуються для формування еталонного і динамічних шаблонів автентифікації для заданої кількості пристроїв.

4. Створення пари приватного і публічного ключів: Сформовані шаблони автентифікації обробляються з використанням алгоритму генерації пари ключів електронного цифрового підпису Лампорта для створення унікальної пари приватного і публічного ключів для створення і перевірки цифрового підпису відповідно для кожного шаблону автентифікації.

5. Створення електронного цифрового підпису до даних: З використанням створеного приватного ключа дані підписуються для формування електронного цифрового підпису. Отриманий цифровий підпис призначений для конкретних даних або цілого повідомлення. Він може бути вбудований у дані або доданих до даних як окремий елемент.

6. Перевірка електронного цифрового підпису: Для перевірки автентичності даних або повідомлення отримувач використовує створений публічний ключ, пов'язаний з використаним приватним ключем, що був застосований для формування електронного цифрового підпису, для перевірки правильності підпису. Якщо перевірка успішна, це підтверджує автентичність відправника та цілісність даних.

7. Перевірка повторного застосування отриманого динамічного шаблону автентифікації: Сформовані динамічні шаблони автентифікації застосовуються одноразово. У випадку повторного застосування того самого шаблону автентифікації, автентифікація електронного пристрою буде відхилена.

8. Перевірка відстані Хемінга для отриманого динамічного шаблону автентифікації: Отриманий динамічний шаблон автентифікації порівнюється з відомим отримувачу еталонним шаблоном автентифікації для обчислення відстані Хемінга. У випадку обчисленого значення відстані Хемінга, що перевищує заданий поріг, автентифікація електронного пристрою буде відхилена.

Створення веб-застосунку дозволяє побудувати модель автентифікації електронних пристроїв, забезпечуючи високий рівень безпеки та надійності для електронної комунікації та обробки даних. Для створення веб-застосунку було обрано програмний каскад Angular завдяки можливості створення компонентів для відображення інтерфейсу користувача, реалізації логіки для генерації пуасонівських імпульсних послідовностей, формування динамічних шаблонів автентифікації та створення і перевірки електронних цифрових підписів, забезпечуючи високий рівень структурованості та підтримки програмного забезпечення.

При успішній перевірці електронного цифрового підпису забезпечується гарантія цілісності повідомлення. Перевірка повторного застосування отриманого динамічного шаблону автентифікації важлива для забезпечення безпеки системи. Цей етап гарантує, що шаблон застосовується лише один раз, унеможливлюючи його повторне використання. Цей етап забезпечує захист проти можливих атак та гарантує одноразовість та унікальність кожної автентифікації, запобігаючи потенційним загрозам безпеки.

Перевірка відстані Хемінга для отриманого динамічного шаблону автентифікації використовується для визначення відмінностей між отриманим шаблоном і відомим еталонним шаблоном. Цей процес гарантує точність та надійність автентифікації, оцінюючи відповідність отриманого динамічного шаблону заздалегідь визначеному еталонному шаблону, що відповідає заданому електронному пристрою

Аналіз результатів

Для перевірки автентичності даних чи повідомлення отримувач використовує створений публічний ключ, пов'язаний із використаним приватним ключем, і у випадку успішної перевірки підпису підтверджується автентичність відправника та цілісність даних. Сформовані динамічні шаблони автентифікації використовуються одноразово, а в разі їхнього повторного застосування автентифікація електронного пристрою буде відхилена. Перевірка відстані Хемінга для отриманого динамічного шаблону, що порівнюється з еталонним шаблоном використовується для визначення відхилення динамічного шаблону автентифікації. У випадку перевищення заданого порогу автентифікація електронного пристрою також буде відхилена. Нижче наведено основні сценарії використання програмної системи згідно описаних вище ключових етапів процесу створення і застосування одноразового електронного цифрового підпису на основі пуасонівських імпульсних послідовностей для автентифікації електронних пристроїв. Для формування шаблонів автентифікації електронного пристрою було згенеровано дві пуасонівські імпульсні послідовності згідно введених параметрів генерації (рис. 5).

Для створених і збережених шаблонів автентифікації отримано пари приватного і публічного ключів (рис. 6). З метою демонстрації роботи етапу моделі автентифікації, приватний і публічний ключ було відображено в програмній моделі із можливістю збереження пари ключів. Із застосуванням збереженого приватного ключа відбувається формування електронного цифрового підпису для повідомлення, що складається з поточного динамічного шаблону автентифікації і публічного ключа з пари для наступного шаблону (рис. 7). Завдяки такому підходу реалізовано механізм ротації ключів.

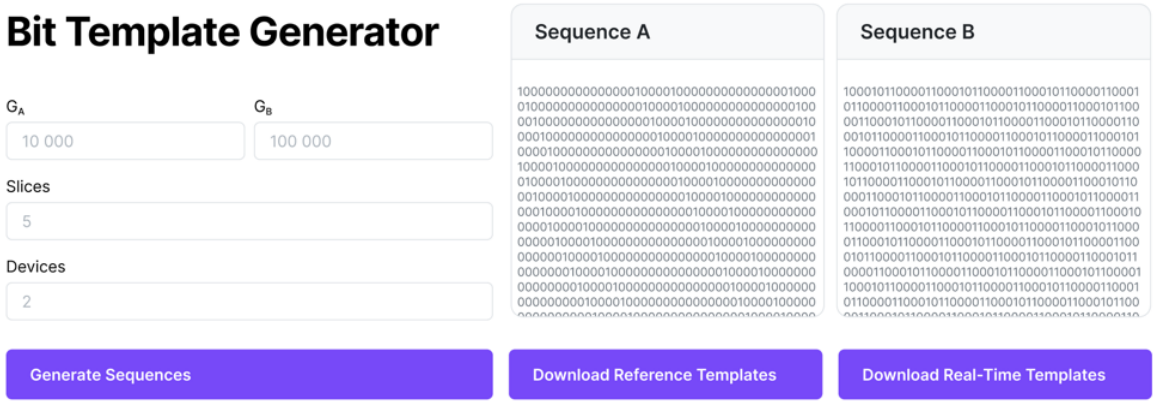

Рис. 5. Результат генерації пуасонівських імпульсних послідовностей для заданих параметрів генерації

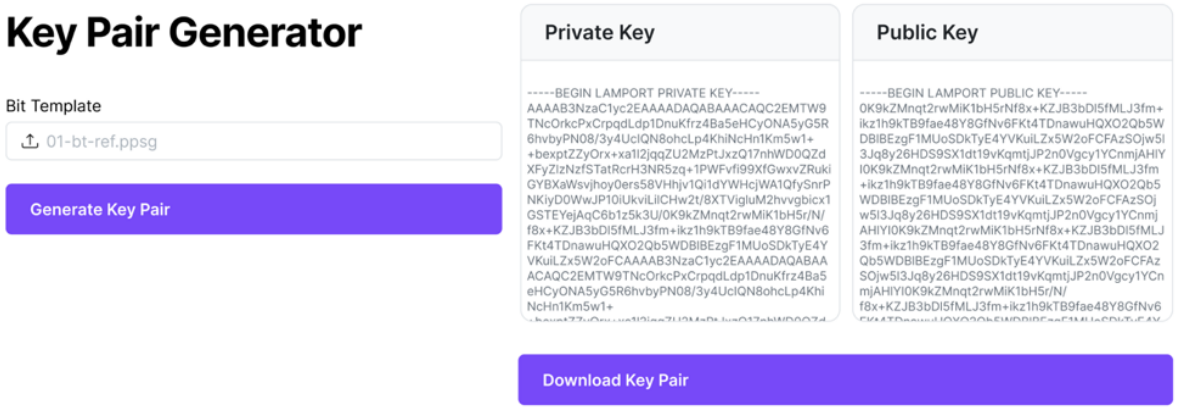

Рис. 6. Результат створення пари приватного і публічного ключів

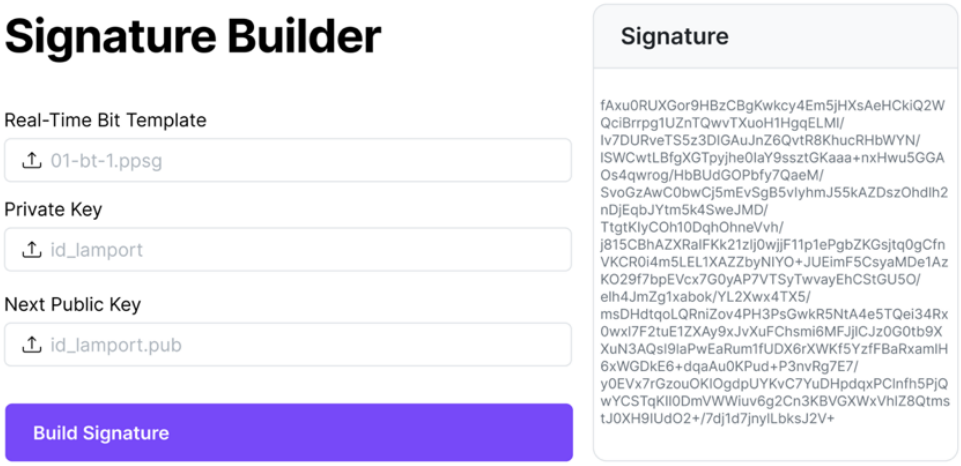

Рис. 7. Результат створення електронного цифрового підпису для збереженого приватного ключа

Сформувавши електронний цифровий підпис, було проведено симуляцію автентифікації електронного пристрою за створеним підписом для різних сценаріїв використання. Нижче наведено результат успішної автентифікації електронного пристрою для створеного електронного цифрового підпису, без модифікації повідомлення і значення підпису, із порівнянням з еталонним шаблоном заданого електронного пристрою (рис. 8).

Наведені вище результати основних сценарії використання програмної системи свідчить про відповідність реалізованої моделі до описаних вище ключових етапів процесу створення і застосування одноразового електронного цифрового підпису на основі пуасонівських імпульсних послідовностей для автентифікації електронних пристроїв.

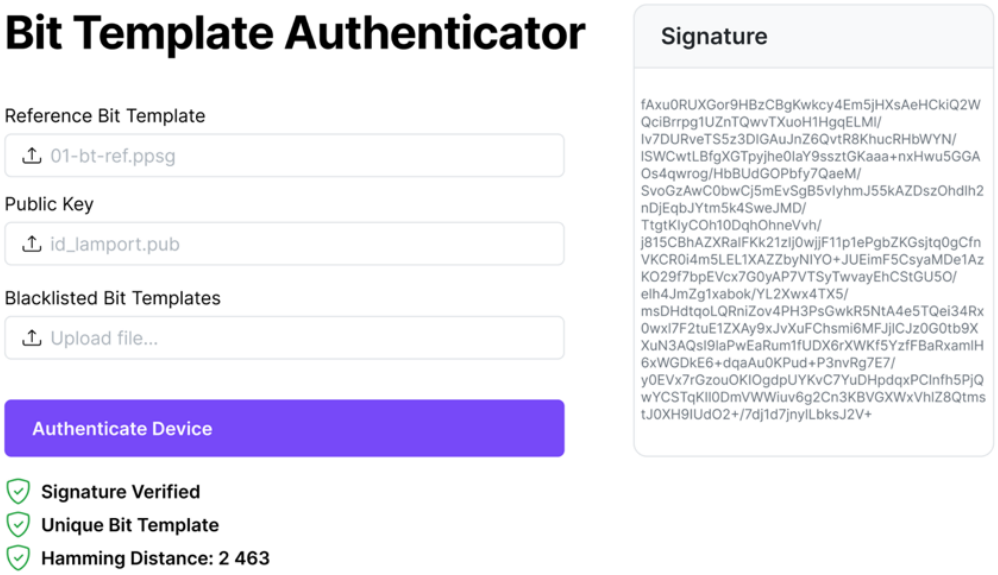

Рис. 8. Результат успішної автентифікації електронного пристрою

Висновки і рекомендації

В результаті виконання дослідження було розкрито сутність основних методів захисту електронного цифрового підпису, їхню ефективність та взаємодію для створення надійної схеми електронного цифрового підпису для автентифікації електронних пристрої із застосуванням динамічних шаблонів автентифікації.

Підхід, що базується на унікальних характеристиках електронних пристроїв через генерацію шаблонів автентифікації, виявив великий потенціал для підвищення рівня безпеки та надійності для процесу автентифікації електронних пристроїв. Ротація ключів, одноразові електронні цифрові підписи та динамічні шаблони автентифікації на основі унікальних характеристик електронних пристроїв є ключовими методами, які забезпечують стійкість електронного цифрового підпису і уможливлюють безпечне застосування ЕЦП в контексті автентифікації електронних пристроїв.

В результаті практичної реалізації моделі автентифікації електронних пристроїв було підтверджено ефективність використання пуасонівських імпульсних послідовностей для формування динамічних шаблонів автентифікації з метою формування електронного цифрового підпису.

На основі проведеного дослідження та практичної реалізації можна розглянути кілька напрямків подальших покращень у розробленій моделі автентифікації електронних пристроїв:

дослідження методів фальсифікації та розробка заходів для їхнього запобігання, проведення детального процесу криптоаналізу;

дослідження альтернативних алгоритмів формування одноразового електронного цифрового підпису для зменшення розмірів пари ключів і підпису;

дослідження можливості застосування запропонованої моделі до децентралізованих систем, наприклад технології блокчейн, для забезпечення необхідного рівня децентралізації і впровадження комунікації між кількома електронними пристроями.

Наведені напрямки покращень розробленої схеми електронного цифрового підпису можуть сприяти не тільки удосконаленню існуючої моделі автентифікації, але й забезпечити можливість до впровадження її в реальні умови в результаті досягнення необхідного рівня криптографічної стійкості і розширення функціональності та універсальності моделі.

Перелік посилань

1. Форми електронного підпису та особливості його використання в захищених інформаційних системах / Паламарчук С., Паламарчук Н., Ткач В., Шугалій О. // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2021. – № 2(14). – С. 100-106.
2. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators / Maksymovych V., Nyemkova E., Justice C., Shabatura M. et al. // Electronics. – 2022. – Vol. 11, № 13. – P. 2039.
3. Erdősi, P. M., Egerszegi, K. Problems in the implementation of the electronic signature // Periodica Polytechnica Social and Management Sciences. – 2003. – № 11. – P. 67–82.
4. Cavus, N., Sancar, N. The Importance of Digital Signature in Sustainable Businesses: A Scale Development Study // Sustainability. – 2023. – Vol. 15, № 6 – P. 5008.
5. Secure Ring Signature Scheme for Privacy-Preserving Blockchain / Wang L., Peng C., Tan W. // Entropy. – 2023. – Vol. 25, № 9. – P. 1334.
6. Making the most of what you have! Profiling biometric authentication on mobile devices / Rasnayaka S., Saha S., Sim T. // 2019 International Conference on Biometrics (ICB), Crete, Greece, June 4-7, 2019. – Piscataway, NJ : IEEE, 2019. – P. 1-7.
7. Nyemkova, E. Authentication of Personal Computers with Unstable Internal Noise // International Journal of Computing. – 2020. – № 19(4). – P. 569-574.
8. The Importance of Key Rotation for Data Security [Electronic resource] / Shiftan A. // Piiano Blog. – 2023. – Web page: https://www.piiano.com/blog/key-rotation (2023).
9. Signing Keys Management – Key Rotation in Depth [Electronic resource] // Cloudentity. – 2023. – Web page: https://cloudentity.com/developers/howtos/auth-settings/signing_keys_management (2023).
10. Towards Practical Post-Quantum Signatures for Resource-Limited Internet of Things / Behnia R., Yavuz A. A. // Annual Computer Security Applications Conference (ACSAC '21), Austin, TX, United States, December 6-10, 2021. – New York, NY: Association for Computing Machinery. – P. 119–130.
11. Порівняльний аналіз одноразових підписів на базі геш-функцій / В. В. Семенець, О. С. Марухненко, І. Д. Горбенко, Г. З. Халімов // Всеукраїнський міжвідомчий науково-технічний збірник «Радіотехніка». – 2020. – № 4(203). – С. 5-18.
12. Lamport signature [Electronic resource] // Wikipedia, the free encyclopedia. – 2023. – Web page: https://en.wikipedia.org/wiki/Lamport_signature (2023).
13. O'Neill, M. E. PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation // ACM Transactions on Mathematical Software. – 2014. – 46 p.

Надійшла 28.04.2024