УДК 004.056.5 DOI: 10.26565/2519-2310-2020-1-05

УДОСКОНАЛЕНА СХЕМА ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ КОДІВ

Олександр Кузнецов[1,2], Анастасія Кіян[2], Тетяна Кузнецова[1]

[1] Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
[2] ПАТ «Інститут інформаційних технологій», вул. Бакуліна, 12, Харків, 61166, Україна
kuznetsov@karazin.ua, nastyak931@gmail.com, kuznetsova.tatiana17@gmail.com

Рецензент: Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський технологічний університет "Шаг", вул. Малом'ясницька, 9/11, Харків, 61010, Україна.
kavserg@gmail.com

Надійшло: Квітень 2020.

Анотація. *Стаття присвячена вивченню та дослідженню властивостей криптосистем на основі кодів. Вони забезпечують високий рівень безпеки навіть в умовах квантового криптографічного аналізу, тобто відносяться до криптосистем нового покоління, до так званих, криптосистем для пост-квантового застосування. Головним недоліком відомих схем цифрового підпису із застосуванням кодів є великий час на формування підпису. Це пов'язано із великою кількістю спроб декодування випадково сформованого вектору (який інтерпретується як синдромний вектор). Висока складність такої процедури вимагає пошуку нових механізмів та алгоритмів, які б прискорили формування електронного підпису за допомогою кодів. У статті представлено результати за двома векторами досліджень. По-перше, ми пропонуємо нову кодову схему цифрового підпису, що базується на використанні однонаправленої функції із класичної криптосистеми Мак-Еліса і не тільки дозволяє забезпечити належний рівень стійкості до класичного криптоаналізу та криптоаналізу із застосуванням квантових компютерів, але і, порівняно із відомими альтернативами,надає захист від атак особливого типу, таких як атака одночасної підробки. Також наводяться кількісні оцінки надійності та швидкості нового криптографічного алгоритму, які отримано шляхом експериментальної перевірки на кодах БЧХ. Другий вектор досліджень стосується дослідження нового напряму, який пов'язаний із модифікацією роботи декодеру шляхом штучного збільшення виправляючої здатності коду. Завдяки вдосконаленій схемі декодування ми можемо значно скоротити час генерації підписів. У роботі підтверджено ефективність застосуванння запропонованої модифікації декодеру алгебраїчних блокових кодів при реалізації нової схеми цифрового підпису у порівнянні із класичним декодером Пітерсона-Горенстейна-Цирлера у контексті порівняння швидкості формування підпису та кількості необхідних спроб декодування.*

Ключові слова: *криптосистеми на кодах, пост-квантова криптографія, електронний підпис, алгебраїчне декодування.*

1 Вступ

У сучасному інформаційному суспільстві важко переоцінити значимість електронного цифрового підпису, що застосовується як для ідентифікації особистості автора, так і для підтвердження цілісності та справжності підписаного ним документа. Це дозволяє надійно використовувати електронний документообіг та отримувати доступ до критично важливих ресурсів [1–3].

На сьогодні у комп'ютерних системах застосовується набір перевірених та стандартизованих на світовому чи державному рівні криптоалгоритмів [4–6]. Однак більшість з подібних схем втратять свою надійність із застосуванням криптоаналізу на повномасштабних квантових комп'ютерах [7–9], розробкою яких займаються ряд компаній зі світовим ім'ям (IBM®, Google® та інші), оскільки подібні методи криптоаналізу здатні вирішувати поширені математичні задачі такі, як дискретне логарифмування чи факторизація, за поліноміальний час. Цей факт призведе до потенційної вразливості не тільки окремих громадян, але і державної електронної документації в цілому [10].

З цієї причини необхідним є всебічне дослідження та аналіз нових методів для формування електронного цифрового підпису, що базуються на принципово інших математичних основах [11]. Подібним перспективним напрямком досліджень пост-квантової криптографії є криптографія, заснована на кодах [12]. Прийнято вважати, що кодова криптографія є ефективною для побудови схем направленого шифрування та інкапсуляції ключів, тоді як для фор-

мування та перевірки цифрового підпису вона не є раціональним рішенням через високу обчислювальну складність [12].

У цілому ряді попередніх робіт [13–15] ми вже розглядали нову кодову схему електронного цифрового підпису (ЕЦП) та довели її ефективності, порівняно з поширеною альтернативою - схемою CFS [16]. Мета цієї роботи полягає в короткому огляді запропонованої схеми та представленню її модифікації із новим декодером, якій дозволяє відчутно знизити обчислювальні затрати на формування підпису, що є вагомим практичним кроком для подолання основного недоліку кодових схем ЕЦП.

2 Кодові схеми ЕЦП

Схема функціонування запропонованої схеми розглядається у якості прикладу роботи кодових схем електронного цифрового підпису, оскільки спільною рисою цих схем є циклічне декодування синдрому задля отримання вектору, що потім стане складовою кінцевого підпису. Повторне декодування є найбільш витратною частиною алгоритму, оскільки зі збільшення кодових параметрів збільшується стійкість схеми, але одночасним є збільшення необхідної кількості спроб для успішного декодування [16].

Запропонована у [13–15] схема цифрового підпису базується на використанні односторонньої функції з класичної криптосистеми Мак-Еліса [17]. Її сутність полягає у інтерпретації гешованого повідомлення у якості кодового слова з помилками, що обчислено згідно двох векторів I та e, які разом зі значенням лічильника складають вихідний підпис.

Розглянемо функціонування схеми, у вигляді чотирьох етапів.

Eman 1. Генерація поля $GF(p^m)$, параметрів коду $m,t \in \mathbb{N}$ та обрання конкретного типу коду, що буде використовуватися.

Eman 2. Формування секретних ключів, що представляють собою матриці X, P, G, які є випадковою невиродженою, переставною та породжуючою матрицею відповідно. Формування відкритого ключа $H_X = X \cdot G \cdot P$.

Eman 3. Формування підпису.

Вхід: повідомлення M, геш-функція h, параметри m,t.

Вихід: підпис у форматі $Y = (I, e, i)$.

1) Обчислюємо геш-значення $h(M)$, згідно обраної на етапі ініціалізації геш-функції. Результатом роботи такої функції є вектор довжини n;

2) Встановлюємо значення лічильника $i = 1$;

3) Знаходимо геш-значення повідомлення $h(M)$, а потім геш-значення $h(h(M) \| i)$, де $\|$ позначає конкатенацію лічильника та геш-значення повідомлення;

4) Тлумачимо $h(h(M) \| i)$ у вигляді кодового слова з помилками $c'_x = (c_0, c_1, ..., c_{n-1})$, на значення якого впливають три фактори: секретний ключ, інформаційне повідомлення $I = (I_0, I_1, ..., I_{k-1})$ та вектор помилок $e = (e_0, e_1, ..., e_{n-1})$, а саме

$$c'_x = I \cdot G_x + e = I \cdot X \cdot G \cdot P + e \ ;$$

5) Множимо знайдене кодове слово на обернену переставну матрицю:

$$c'_x \cdot P^{-1} = I \cdot X \cdot G \cdot P \cdot P^{-1} + e \cdot P^{-1} = I \cdot X \cdot G + e \cdot P^{-1} \ .$$

Отриманий результат представляє з собою кодове слово, що викривлене не більше, ніж в t розрядах. По відношенню до нього можна застосувати алгоритм швидкого декодування для отримання необхідних векторів I та e.

6) Декодуємо отримане кодове слово $c'_x = (c_0, c_1, ..., c_{n-1})$:

- Якщо декодування вдале, продовжуємо обчислення;
- Якщо декодування невдале, збільшуємо значення лічильника на 1, та повторюємо кроки №№ 3-6;

7) Декодування дозволило отримати вектори $I' = I \cdot X$ та $e' = e \cdot P^{-1}$;

8) Обчислюємо вектори $I' \cdot X^{-1} = I$ та $e' \cdot P = e$;

9) Формуємо підпис: $Y=(I,e,i)$.

Декодування кодового слова для уповноваженого користувача, як і декодування синдромної послідовності, є задачею поліноміальної складності. Для неуповноваженого користувача напроти *NP*–складною задачею, розв'язання якої обчислювально недосяжне за нормальних умов.

Етап 4. Перевірка підпису.

Вхід: повідомлення M, підпис $Y=(I,e,i)$, геш-функція h, відкритий ключ G_x.

Вихід: висновок про коректність підпису.

Сутність перевірки підпису полягає у перевірці факту, чи інтерпретація геш-функції у якості кодового слова з помилками обчислена за переданим у підписі вектором помилок $e=(e_0,e_1,...,e_{n-1})$ та вектором $I=(I_0,I_1,...,I_{k-1})$. Для того, щоб здійснити подібну перевірку, необхідно:

1. Знайти геш-значення $s'_x=h(h(M)\|i)$;
2. Обчислити вектору $s''_x=I\cdot G_x+e$;
3. Порівняти отримані s'_x та s''_x. Якщо вектори збігаються, то можливо зробити висновок про коректність підпису. В іншому випадку-підпис відхиляється.

Очевидним є той факт, що найбільше часу серед представленого алгоритму формування підпису, вимагає саме крок повторного декодування синдрому. І ефективність процедури декодування напряму залежить від типу використовуваного декодеру. Нижче розглянемо типовий декодер, що використовує схеми кодового цифрового підпису, а також нову - модифіковану схему декодеру, яка дозволяє суттєво оптимізувати процес.

3 Удосконалена схема електронного підпису на кодах

На сьогодні найбільш поширеними кодами, що застосовуються при реалізації кодових схем ЕЦП є коди Гоппа та коди БЧХ [12,16,18]. Нижче розглянемо останню модифікацію відповідних схем. Відомо, що коди БЧХ відносять до класу циклічних кодів і з цієї причини вони можуть бути декодовані методами, що застосовуються до декодування циклічних кодів, а також із застосуванням спеціально розроблених методів, зокрема метод на основі рішення ключового рівняння [19–21]. Сутність цього методу полягає у знаходженні многочлену локаторів помилок. З цією метою можуть бути застосовані лише три метода: алгоритм Пітерсона, алгоритм Евкліда та алгоритм Берлекемпа-Мессі [19, 20].

Найбільш універсальним при цьому є алгоритм Пітерсона, що дозволяє виконати декодування, як у двійковому, так і у недвійковому випадку, на відміну від своїх альтернатив, які потребують для недвійкового випадку проведення додаткових етапів. Докладно алгоритм Пітерсона представлено у роботах [19–21]. Спираючись на такі міркування, вважаємо за можливе запропонувати власну, модифіковану конфігурацію декодера, яка може бути застосована для оптимізації обчислень кодових схем цифрового підпису.

Як відомо, для коректного формування підпису важливим є сам факт правильності декодування синдромної послідовності, а не те, у який вектор вона декодується. З цієї причини сутність запропонованої схеми декодера полягає у штучному збільшенні виправляючої здатності коду t, без зміни інших кодових параметрів. Цей факт дозволить збільшити кількість дозволених комбінацій, у які може декодуватися синдромна послідовність.

Припустимо, що задано код $(n,k,d=2t+1)$. На вхід декодеру подається послідовність довжини $n-k$. У полі $GF(2^m)$ кількість можливих послідовностей дорівнює 2^{n-k}. На виході декодеру має бути отримано послідовність довжини n, при чому кількість помилок має не перевищувати виправлячу здатність коду t. Всього можливих конфігурацій помилок C_n^t. Таким чином ймовірність успішного декодування можна визначити як відношення кількості можливих наборів помилок до загальної кількості вхідних синдромів:

$$P = \frac{C_n^t}{2^{n-k}} .$$

Узагальнений алгоритм декодера можна представити у вигляді наступних кроків:

1. На вхід декодеру поступає значення виправляючої здатності коду t, коефіцієнт штучного збільшення виправляючої здатності η та кодова комбінація $c'(x) = c(x) + e(x)$, де $c(x)$ - це передана комбінація, у якій під час передачі виникли помилки, що представлені у вигляді многочлену $e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + ... + e_{i_v} x^{i_v}$, де $0 \le v \le t$ представляє собою кількість помилок, e_{i_k} -значення помилки, i_k - номер позиції, в якій відбулася помилка. Для того, щоб виправити помилку, необхідно визначити e_{i_k} та i_k;

2. Встановити кількість рівнянь $v = t$ рівною значенню виправляючої здатності коду;

3. Обчислити синдроми $s(x) = s_1 x^0 + s_2 x^l + ... + s_{n-k} x^{n-k-l}$, де коефіцієнти s_i визначаються підстановкою у $c(x)$ коренів α^i породжуючого многочлена коду;

4. Інтерпретувати обчислені синдроми у вигляді матриці при $\mu = v$

$$M = \begin{bmatrix} s_1 & s_2 & s_\mu \\ s_2 & s_3 & s_{\mu+1} \\ \dots & \dots & \dots \\ s_\mu & s_{\mu+1} & s_{2\mu-1} \end{bmatrix}.$$

Матриця є невиродженою, якщо виникло рівно t помилок, у іншому випадку матриця є виродженою і у цьому випадку детермінант матриці дорівнює 0, та необхідно повторити кроки №№ 2-4 для $v = v - 1$;

5. Синтезувати многочлен локаторів помилок $\lambda(x)$ згідно із знайденими попередньо коефіцієнтами. Визначення коефіцієнтів многочлена локаторів помилок в алгоритмі Пітерсона зводиться до рішення v лінійних рівнянь з v невідомими коефіцієнтами λ_k;

6. Обчислити локатори x_i многочлена $\lambda(x)$ за допомогою процедури Ченя: послідовне обчислення $\lambda(\alpha^j)$ для кожного можливого j та перевірка отриманих значень на нуль. Якщо $\lambda(\alpha^{-k})$ дорівнює нулю, то α^k є локатором помилки;

7. Знайти синдроми s'_x згідно многочлену локаторів помилок;

8. Перевірити рівність векторів $s_x = s'_x$:
   - Якщо вектори рівні, то декодування вдале і декодування завершується;
   - Якщо вектори відрізняються, то збільшуємо значення виправляючої здатності коду $t = t + 1$ та повторюємо кроки №№ 1-7 до тих пір, поки декодування не буде вдалим, або поки значення виправляючої здатності не досягне значення, заданого коефіцієнтом збільшення.

4 Експериментальні дослідження

З метою дослідження особливостей функціонування запропонованого декодеру було синтезовано відповідні реалізації схеми CFS [16] та розглянутої вище схеми, з урахуванням декодеру Пітерсона і запропонованого нами декодеру на мові програмування Java. Проведене моделювання підтвердило теоретичні твердження [13–15], а саме, що практичні результати експериментів для схеми CFS та запропонованої схеми є еквівалентними. Враховуючи цю обставину наведемо результати експериментів лише для запропонованої схеми.

Експеримент №1.

Вхідні дані: код $(n, k, d = 2t + 1)$, $n = 255$, параметр t змінюється від 1 до 11 з кроком 1. У залежності від параметра t відповідно змінюється і параметр k. Використовується зви-

чайний (відомий) декодер. Результати наведено у таблиці 1.

Таблиця 1 – Результати експерименту №1

n	k	t	Час підпису, mc	Кількість спроб для успішного декодування
255	247	1	196	1
255	239	2	43	1
255	231	3	30	4
255	223	4	160	42
255	215	5	460	213
255	207	6	2043	1356
255	199	7	739	417
255	191	8	432499	262670
255	187	9	15874	8355
255	179	10	1681908	781048

Вихідні дані: кількість спроб для успішного декодування та значення швидкості формування підпису.

Експеримент №2.

Вхідні дані: код $(n,k,d=2t+1)$, $n=255$, параметр t змінюється від 1 до 11 з кроком 1. У залежності від параметра t відповідно змінюється і параметр k. Використовується новий декодер зі збільшенням t на 2 та коефіцієнтом $\eta=0.7$. Результати наведено у таблиці 2.

Таблиця 2 – Результати експерименту №2

n	k	t	Час підпису, mc	Кількість спроб для успішного декодування
255	247	1	147	1
255	239	2	50	2
255	231	3	32	1
255	223	4	122	11
255	215	5	75	8
255	207	6	2241	732
255	199	7	8624	2615
255	191	8	14922	4128
255	187	9	139732	30101
255	179	10	147717	31476

Вихідні дані: кількість спроб для успішного декодування та значення швидкості формування підпису.

Експеримент №3.

Вхідні дані: код $(n,k,d=2t+1)$, $n=255$, параметр t змінюється від 1 до 11 з кроком 1. У залежності від параметра t відповідно змінюється і параметр k. Використовується новий декодер зі збільшенням t на 4 та коефіцієнтом $\eta=0.7$. Результати наведено у таблиці 3.

Вихідні дані: кількість спроб для успішного декодування та значення швидкості формування підпису.

Відобразимо отримані дані моделювання у вигляді відповідних залежностей часу підпису від коректуючої здатності коду та кількості спроб для успішного декодування (див. Рис. 1-2). Отримані залежності представлені у логарифмічному масштабі за віссю ординат. Розрахунок логарифмічного значення здійснено згідно з формулою: $y=\lfloor \log_{10} y' \rfloor$, де символ $\lfloor\ \rfloor$ - позначає округлення значення до найменшого цілого.

Таблиця 3 – Результати експерименту №3

n	k	t	Час підпису, mc	Кількість спроб для успішного декодування
255	247	1	197	1
255	239	2	60	1
255	231	3	46	3
255	223	4	78	5
255	215	5	741	121
255	207	6	1717	368
255	199	7	16513	3373
255	191	8	63055	11262
255	187	9	138325	24848
255	179	10	1532886	197837

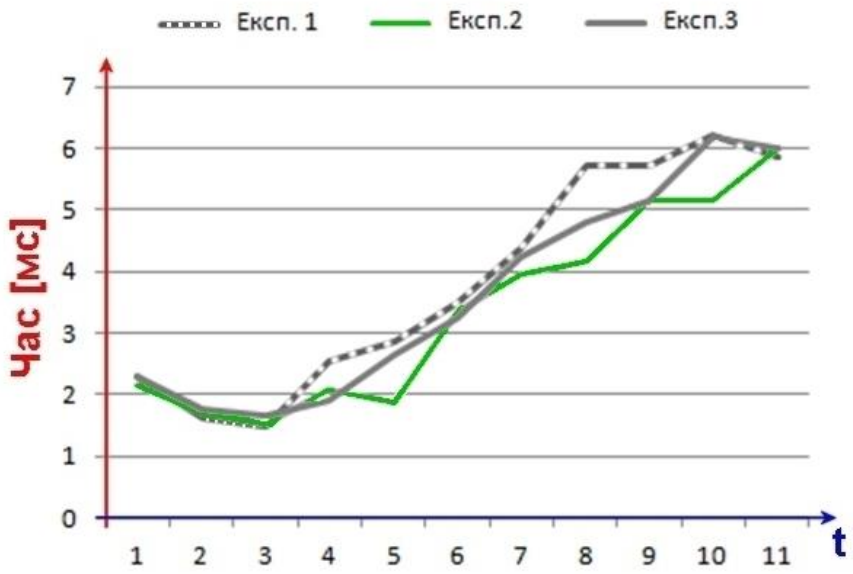

Рис. 1 – Швидкість формування підпису з використанням різних декодерів

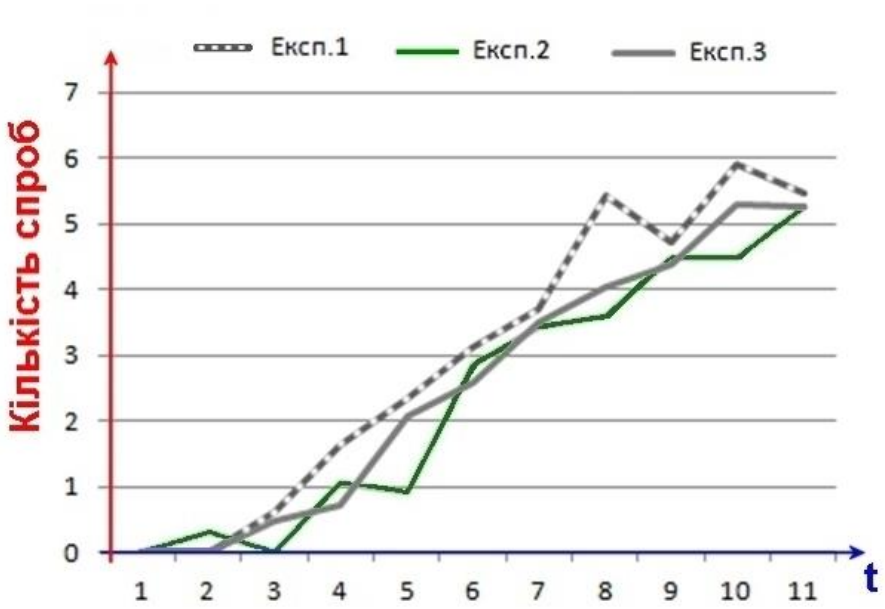

Рис. 2 – Кількість спроб для успішного декодування
з використанням різних декодерів

Змінний характер графіків швидкості пояснюється залежністю швидкості від кількості спроб, які необхідні для успішного декодування, а також завантаженістю обчислювальної платформи, яка вносить похибку. Більш об'єктивним є показник кількості спроб декодування. Так, якщо ми збільшимо параметр t на 1, то це автоматично збільшить кількість можливих конфігурацій помилок у

$$\frac{C_n^{t+1}}{C_n^t} = \frac{n!t!(n-t)!}{(t+1)!\cdot(n-t-1)!n!} = \frac{n-t}{t+1}$$

разів. Звідси, збільшення загальної ймовірності декодування буде відбуватися поки $n-t > t+1$, тобто $t < \frac{n+1}{2}$. Для обмеження даної величини в роботу декодеру було введено додатковий параметр, коефіцієнт збільшення t, аби запобігти випадкам нераціонального виконання алгоритму.

Спираючись на аналіз отриманих результатів моделювання, можна зробити висновок, що застосування запропонованого декодеру дозволяє зменшити час, якій необхідний для формування підпису. Цей ефект досягається за рахунок того, що дообчислення додаткових синдромів та повторне декодування потребують меншої кількості обчислень, ніж збільшення лічильника і виконання усіх кроків: - від гешування значень до декодування.

5 Висновки

Кодова криптографія є одним з найбільш перспективних напрямків розвитку пост-квантової криптографії, особливо у контексті реалізації схем направленого шифрування та інкапсуляції ключів. Однак, цей напрямок криптографії рідко розглядають як альтернативу для реалізації пост-квантового цифрового підпису через високу обчислювальну складність алгоритму формування ЕЦП. Ця складність, перш за все, обумовлена складністю циклічного декодування синдрому, оскільки етап декодування в алгоритмах формування цифрового підпису вимагає найбільшу кількість обчислень. При цьому ефективність декодування напряму залежить від використовуваного декодеру.

В даній роботі авторами запропоновано та досліджено принципово новий тип декодеру, що реалізує штучне збільшення значення виправляючої здатності після невдалого декодування та повторному декодуванні синдрому. Такий принцип роботи дозволяє збільшити ймовірність успішного декодування через збільшення кількості можливих наборів помилок по відношенню до загальної кількості вхідних синдромів.

Проведені практичні дослідження довели, що застосування запропонованої схеми роботи декодеру, порівняно із типовим декодером циклічних кодів Пітерсона, дозволяє значно зменшити кількість спроб, необхідних для декодування синдрому, і таким чином зменшити час, що вимагає алгоритм формування цифрового підпису. Зменшення часових витрат обумовлюється тим, що дообчислення додаткових синдромів і повторне декодування потребують меншої кількості обчислень, ніж збільшення значення лічильника та повторне виконання усіх кроків від гешування значень до декодування.

Подібна, удосконалена схема декодеру може бути застосована не тільки до розглянутого конкретного прикладу запропонованої кодової схеми підпису, але і для усіх схем цифрового підпису, що базуються на використанні циклічних кодів.

Подальшим напрямком досліджень є вивчення можливостей застосування запропонованого підходу до інших класів кодів, зокрема, до кодів Гоппи, на яких будується більшість надійних та безпечних кодових криптосистем [12, 22].

Посилання

[1] Padhye S. et al. Digital Signature [Electronic resource] // Introduction to Cryptography. CRC Press, 2018. P. 205–222. URL: https://www.taylorfrancis.com/ (accessed: 16.07.2020).

[2] Priyadarshini S.B.B. et al. Digital Signature and Its Pivotal Role in Affording Security Services [Electronic resource] // Handbook of e-Business Security. Auerbach Publications, 2018. P. 365–384. URL: https://www.taylorfrancis.com/ (accessed: 16.07.2020).

[3] Martin K.M. Digital Signature Schemes. Oxford University Press, 2017. Vol. 1.
[4] Rubinstein-Salzedo S. Cryptography. Cham: Springer International Publishing, 2018.
[5] Klima R.E. et al. Cryptology : Classical and Modern. Chapman and Hall/CRC, 2018.
[6] Martin K. Everyday Cryptography. Oxford University Press, 2017. Vol. 1.
[7] National Academies of Sciences E. Quantum Computing: Progress and Prospects. 2018.
[8] Aaronson S. Quantum computing and hidden variables // Phys. Rev. A. 2005. Vol. 71, № 3. P. 032325.
[9] Preskill J. Quantum Computing in the NISQ era and beyond // Quantum. 2018. Vol. 2. P. 79.
[10] Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings / ed. Ding J., Tillich J.-P. Cham: Springer International Publishing, 2020. Vol. 12100.
[11] Computer Security Division I.T.L. Post-Quantum Cryptography | CSRC | CSRC [Electronic resource] // CSRC | NIST. 2017. URL: https://content.csrc.e1c.nist.gov/Projects/Post-Quantum-Cryptography/faqs (accessed: 16.07.2020).
[12] Overbeck R., Sendrier N. Code-based cryptography // Post-Quantum Cryptography / ed. Bernstein D.J., Buchmann J., Dahmen E. Berlin, Heidelberg: Springer, 2009. P. 95–145.
[13] Kuznetsov A. et al. Code-based electronic digital signature // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2018. P. 331–336.
[14] Kuznetsov A. et al. New Approach to the Implementation of Post-Quantum Digital Signature Scheme // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2020. P. 166–171.
[15] Kuznetsov A. et al. Code-Based Schemes for Post-Quantum Digital Signatures // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2019. Vol. 2. P. 707–712.
[16] Courtois N.T., Finiasz M., Sendrier N. How to Achieve a McEliece-Based Digital Signature Scheme // Advances in Cryptology — ASIACRYPT 2001 / ed. Boyd C. Berlin, Heidelberg: Springer, 2001. P. 157–174.
[17] McEliece R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory // Deep Space Netw. Prog. Rep. 1978. Vol. 44. P. 114–116.
[18] Finiasz M. Parallel-CFS // Selected Areas in Cryptography / ed. Biryukov A., Gong G., Stinson D.R. Berlin, Heidelberg: Springer, 2011. P. 159–170.
[19] Blahut R.E. Theory and Practice of Error Control Codes. Reprint. with corr edition. Reading, MA: Addison-Wesley, 1983. 500 p.
[20] The Theory of Error-Correcting Codes. Elsevier, 1977. Vol. 16.
[21] Clark G.C., Cain J.B. Error-Correction Coding for Digital Communications. Boston, MA: Springer US, 1981.
[22] Kuznetsov A. et al. Code-based public-key cryptosystems for the post-quantum period // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). 2017. P. 125–130.

Рецензент: Сергей Кавун, доктор экономических наук, к.т.н., проф., Харьковский технологический университет "ШАГ", ул. Маломясницкая, 9/11, Харьков, 61010, Украина.
E-mail: kavserg@gmail.com

Поступила: Апрель 2020.

Авторы:

Александр Кузнецов, д.т.н., проф., ХНУ имени В.Н. Каразина, Харьков, 61022, Украина.
E-mail: kuznetsov@karazin.ua

Анастасия Киян, аналитик по системам защиты информации. АО "Институт информационных технологий", ул. Бакулина, 12, Харьков, 61166, Украина.
E-mail: nastyak931@gmail.com

Татьна Кузнецова, научный сотрудник, ХНУ имени В.Н. Каразина, Харьков, 61022, Украина.
E-mail: kuznetsova.tatiana17@gmail.com

Усовершенствованная схема электронной цифровой подписи на основе кодов.

Аннотация. Статья посвящена изучению и исследованию свойств криптосистем на основе использования кодов. Они обеспечивают высокий уровень безопасности даже в условиях квантового криптографического анализа, то есть относяться к криптосистем нового поколения, к так называемым, криптосистемам для пост-квантового применения. Главным недостатком известных схем цифровой подписи с использованием кодов является большое время, требуемое для формирования подписи. Это связано с большим количеством попыток декодирования случайно сформированного вектора (который интерпретируется как синдромный вектор). Высокая сложность такой процедуры требует поиска новых механизмов и алгоритмов, которые способны ускорить формирование электронной подписи. В статье представлены результаты согласно двух векторов исследований. Во-первых, мы предлагаем новую кодовую схему цифровой подписи, которая основана на использовании однонаправленной функции из классической криптосистемы Мак-Элиса и не только позволяет обеспечить надлежащий уровень устойчивости к классическому криптоанализу и криптоанализу с применением квантовых компьютеров, но и по сравнению с известными альтернативами, предоставляет защиту от атак особого типа, таких как атака одновременной подделки. Также приводятся количественные оценки надежности и скорости нового криптографического алгоритма, полученные путем экспериментальной проверки реализаций на кодах БЧХ. Второй вектор исследований касается исследования нового направления, связанного с модификацией работы декодера алгебраических блоковых кодов путем искусственного увеличения исправляющей способности кода. Благодаря усовершенствованной схеме декодирования мы можем значительно сократить время генерации подписей. В работе подтверждена эффективность применения предлагаемой модификации декодера при реализации новой схемы цифровой подписи по сравнению с классическим декодером Питерсона-Горенстейна-Цирлера в контексте сравнения скорости формирования подписи и количества необходимых попыток декодирования.

Ключевые слова: криптосистемы на кодах, пост-квантовая криптография, электронная подпись, алгебраическое декодирование.

Reviewer: Serhii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Kharkiv University of Technology "STEP", Malom'yasnitska St. 9/11, Kharkiv, 61010, Ukraine. Ï
E-mail: kavserg@gmail.com

Received on April 2020.

Authors:
Alexandr Kuznetsov, Doctor of Sciences (Eng.), Full Prof., V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsov@karazin.ua
Anastasiia Kiian, information security analyst, JSC "Institute of Information Technologies", Kharkiv, 61166, Ukraine
E-mail: nastyak931@gmail.com
Tatyana Kuznetsova, Researcher, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsova.tatiana17@gmail.com

Advanced code-based electronic digital signature scheme.

Annotation. The article is devoted to the study and research of the properties of code-based cryptosystems. They provide a high level of security even in the conditions of quantum cryptographic analysis, i.e. belong to the new generation of cryptosystems for post-quantum application. The main disadvantage of the known code-based digital signature schemes is the long time to generate a signature. This is due to the large number of attempts to decode a randomly generated vector (which is interpreted as a syndrome vector). The high complexity of such a procedure requires the search for new mechanisms and algorithms that would accelerate the formation of code-base electronic signatures. The article presents the results of two research vectors. First, we propose a new code-based digital signature scheme on the use of a one-way function from the classical McEliece cryptosystem and not only provides a proper level of resistance to classical cryptanalysis and cryptanalysis using quantum computers, but also, compared to known alternatives, provides protection against special types of attacks, such as simultaneous counterfeit attacks. Quantitative estimates of the reliability and speed of the new cryptographic algorithm, which were obtained by experimental verification on the BCH codes, are also given. The second vector of research concerns the study of a new direction, which is associated with the modification of the decoder by artificially increasing the corrective code ability. Thanks to the improved decoder scheme, we can significantly reduce the generation time of signatures. The paper confirms the effectiveness of the proposed decoder modification in the implementation of a new digital signature scheme in comparison with the classic Peterson-Gorenstein-Zierler decoder in the context of comparing the speed of signature formation and the number of required decoding attempts.

Key words: Cryptosystems on codes; Post-quantum cryptography; Electronic signature; Algebraic decoding.