

УДК 004.056.5

Гриценко І.Д.¹, Козіна Г.Л.²

¹ студ.гр. РТ-818 НУ «Запорізька політехніка»

² канд. фіз.-матем. наук, доц. НУ «Запорізька політехніка»

АЛГОРИТМ ЦИФРОВОГО ПІДПISУ З ВИКОРИСТАННЯМ АЛГЕБРАЇЧНОГО КОДУВАННЯ

Для формування цифрового підпису на сьогоднішній день використовуються криптографічні механізми та протоколи, у яких завдання пошуку секретного ключа за відомим відкритим ключем пов'язане з вирішенням відомої та надзвичайно складної математичної задачі (наприклад, факторизації, дискретного логарифмування, дискретного логарифмування в групі точок еліптичної кривої).

Однак квантові обчислення дозволяють суттєво прискорити вирішення багатьох математичних завдань. Наприклад, алгоритм Шора дозволяє знайти за прийнятний час усі прості множники у системі RSA, тобто. знайти секретний ключ та/або підробити цифровий підпис без знання секретного ключа.

У цьому сенсі розробка, дослідження та обґрунтування рекомендацій щодо практичного використання нових криптосистем, стійких до квантового криптоаналізу, має особливу актуальність та затребуваність

Один із напрямків у розвитку постквантової криптографії ґрунтується на використанні алгебраїчних блокових кодів (Code-based Cryptography) [1]. При цьому забезпечується висока швидкість криптографічного перетворення, стійкість до класичного і квантового криптоаналізу, а також можливість додаткового контролю помилок.

В основі побудови кодових криптосистем лежить використання спеціальних маскуючих матриць, які виступають як секретний ключ і, за припущенням, надійно приховують алгебраїчну структуру коду.

Зловмисник, не знаючи секретного ключа, не може скористатися алгебраїчним алгоритмом декодування поліноміальної складності і змушений декодувати кодове слово, вирішуючи складне NP-завдання (non-deterministic polynomial).

Алгоритм формування та перевірки цифрового підпису з використанням алгебраїчних кодів заснований на криптосистемі Нідеррайтера [2,3] і був представлений Courtois, Finiasz та Sendrier.

Оцінка стійкості цієї схеми (названої за ініціалами її винахідників – CFS) проти підробки підпису може бути зведена до оцінки складності розв'язання задач синдрому декодування. Знання секретного ключа дозволяє декодеру вирішити це завдання для певної частки випадкових кодових слів.

В схемі CFS для формування цифрового підпису реалізується багаторазове хешування інформативного повідомлення, рандомізованого лічильником бітової довжини r , до тих пір, поки не буде отримано правильно виділений синдром (що допускає декодування). Уповноважений користувач використовує секретний ключ для визначення відповідного вектору помилок. Разом з поточним значенням лічильника цей вектор помилок використовується як підпис.

Реалізація схеми CFS для формування та перевірки цифрового підпису здійснюється у відповідності з наступним алгоритмом [4].

1. Генерація загальносистемних параметрів: вибираються позитивні цілі числа m, t .

2. Генерація ключа: формуються пари ключів як у криптосистемі Нідеррайтера на основі алгебраїчного коду з класу $(n = 2^m, k = n - mt, 2t + 1)$ двоїчних кодів Гоппи.

Для цього формуються: матриця $A: (n - k) \times n$, матриця $X: (n - k) \times (n - k)$, матриця $P: m \times n$.

Відкритим ключем є матриця $H_x = X \times H \times P$ та число t (Здатність коду на виправлення). Секретним ключем є матриці H, X та P а також пов'язаний з матрицею H швидкий (поліноміальна складність) алгоритм декодування алгебраїчного коду.

Алгоритм декодування дозволяє за введеною синдромною послідовністю $S = (s_0, s_1, \dots, s_{n-k-1})$ у разі успіху декодування знайти вектор помилок $e = (e_0, e_1, \dots, e_{n-1})$ та кодове слово $c = (c_0, c_1, \dots, c_{n-1})$.

В іншому випадку (якщо декодування не вдалося) алгоритм видає відмову в обробці синдрому $S = (s_0, s_1, \dots, s_{n-k-1})$, тобто. за такою послідовністю алгоритм не може знайти вектор помилок $e = (e_0, e_1, \dots, e_{n-1})$ та кодове слово $c = (c_0, c_1, \dots, c_{n-1})$.

3. Формування підпису.

Вхід: h – функція хешування, яка застосовується до вхідних даних x (аргументу функції) довільної довжини, результатом хешування є хеш-код $h(x)$ довжини $n - k$ біт; швидкий (поліноміальної складності) алгоритм декодування алгебраїчного коду, який застосовується до синдромної послідовності $S = (s_0, s_1, \dots, s_{n-k-1})$.

Припускається, що в результаті виконання алгоритму декодування можливі дві ситуації: якщо декодування успішне – виводиться знайдений вектор помилок $e = (e_0, e_1, \dots, e_{n-1})$, який відповідає вектору $S = (s_0, s_1, \dots, s_{n-k-1})$, якщо декодування не успішне – видається повідомлення про неможливість знайти вектор помилок $e = (e_0, e_1, \dots, e_{n-1})$ для введеного вектору $S = (s_0, s_1, \dots, s_{n-k-1})$; відкритий текст M , для якого необхідно сформулювати цифровий підпис за схемою CFS.

Вихід: цифровий підпис Y за схемою CFS для відкритого тексту M .

Алгоритм формування цифрового підпису за схемою CFS.

Крок 1. Хешування відкритого тексту M , тобто обчислення хеш-коду $h(M)$. Привласнення змінної i значенню $i = 1$;

Крок 2. Обчислення хеш-коду $h(h(M) || i)$, де $h(M) || i$ – конкатенація (об'єднання) значень $h(M)$ та i представлених у вигляді бітових послідовностей;

Крок 3. Значення $h(h(M) || i)$ інтерпретується як синдромна послідовність $s_i = (s_{i0}, s_{i1}, \dots, s_{i(n-k-1)})$, обчислена для деякого (довільного) кодового слова та вектора помилок $e = (e_0, e_1, \dots, e_{n-1})$, тобто передбачається виконання рівності для відкритого ключа $H_x = X \times H \times P$.

Крок 4. Обчислення значення вектору

$$S_i^T = X^{-1} \times s_i^T \quad (1)$$

який (як передбачається) є синдром, обчислений за перевіркою матрицею H алгебраїчного (n, k, d) коду, тобто. передбачається, що

$$S_i^T = X^{-1} \times s_i^T = X^{-1} \times H_x \times e^T = H \times P \times e^T = H \times e^T \quad (2)$$

та алгоритм швидкого декодування дозволить знайти вектор $e^{-T} = P \times e^T$.

Крок 5. Для синдромної послідовності s_x^* реалізується виконання швидкого алгоритму декодування.

Якщо декодування успішне – виводиться знайдений вектор помилок $e^{-T} = P \times e^T$, який відповідає вектору s_x^* .

Якщо декодування не успішне – видається повідомлення про неможливість знайти вектор помилок $e^{-T} = P \times e^T$ для вектора s_x^* . В цьому випадку змінною i присвоюється значення $i = i + 1$ здійснюється перехід на Крок 2.

Крок 6. Обчислення вектору

$$e^T = P^{-1} \times e^{-T} = P^{-1} \times P \times e^T \quad (3)$$

Крок 7. Формування цифрового підпису за схемою CFS $Y = (a, f)$, для відкритого тексту M .

Алгоритм верифікації (алгоритм перевірки цифрового підпису за схемою CFS)

Крок 1. Обчислення вектору

$$(s_x^1)^T = H_x \times e^T \quad (4)$$

Крок 2. Прийняття рішення про справжність або несправжність цифрового підпису

$$(s_x^1)^T = h(h(M) || f) \quad (5)$$

Якщо $s_x^1 = s_x^1$, тоді приймається рішення про справжність справжність цифрового підпису.

Якщо $s_x^1 \neq s_x^1$, тоді приймається рішення про несправжність цифрового підпису.

Крок 3. Прийняття рішення про справжність або несправжність цифрового підпису.

Якщо $s_x^1 = s_x^1$ та $w(e) \leq t$ тоді приймається рішення про справжність цифрового підпису.

Якщо $s_x^1 \neq s_x^1$ та (або) $w(e) > t$ тоді приймається рішення про несправжність цифрового підпису.

Додаткова перевірка ваги Хеммінгу вектору e дозволяє захиститися від підробки підпису з урахуванням додавання довільного кодового слова.

У роботі розглянуто та програмно реалізовано алгоритм цифрового підпису з використанням алгебраїчного кодування за схемою CFS, а також алгоритм верифікації за схемою CFS.

В якості вхідних параметрів було обрано матриця H порядку 4×7 , матриця X порядку 4×4 та матриця P порядку 7×7 . В якості функції хешування обрано CRC32.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Raphael O., Sendrier N. Code-based cryptography. [Електронний ресурс]. – Режим доступу: https://link.springer.com/chapter/10.1007/978-3-540-88702-7_4
2. Niederreiter cryptosystem. [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Niederreiter_cryptosystem
3. Niederreiter, H. Knapsack-type Cryptosystems And Algebraic Coding Theory // Problem Control and Inform Theory, 1986, v. 15. P. 19-34. Режим доступу: <https://vdoc.pub/documents/knapsack-type-cryptosystems-and-algebraic-coding-theory-2tgbc23plpdg>.
4. Кузнецов А. А. Алгоритмы электронной цифровой подписи на основе алгебраического кодирования / А.А. Кузнецов, А.И. Пушкарев, А.С. Киян // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 59–74. – Режим доступу: <https://openarchive.nure.ua/handle/document/4328>.