



УКРАЇНА

(19) **UA** (11) **116152** (13) **U**  
(51) МПК (2017.01)**H03M 13/00****H03M 13/19** (2006.01)**G06F 21/64** (2013.01)**G06F 17/16** (2006.01)ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ**(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ****(21)** Номер заявки: **u 2016 11784****(22)** Дата подання заявки: **21.11.2016****(24)** Дата, з якої є чинними  
права на корисну  
модель: **10.05.2017****(46)** Публікація відомостей  
про видачу патенту: **10.05.2017, Бюл.№ 9****(72)** Винахідник(и):**Кузнецов Олександр Олександрович**  
**(UA),****Пушкаръов Андрій Іванович (UA),****Сватовський Ігор Іванович (UA),****Шевцов Олексій Володимирович (UA),****Кузнецова Тетяна Юріївна (UA)****(73)** Власник(и):**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ****УНІВЕРСИТЕТ ІМЕНІ В.Н. КАРАЗІНА,****пл. Свободи, 4, м. Харків, 61022 (UA)****(54) СПОСІБ ФОРМУВАННЯ ТА ПЕРЕВІРКИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ІЗ ВИКОРИСТАННЯМ АЛГЕБРАЇЧНИХ БЛОКОВИХ КОДІВ****(57)** Реферат:

Спосіб формування та перевірки електронного цифрового підпису із використанням алгебраїчних блокових кодів полягає в тому, що лінійний алгебраїчний блоковий  $(n, k, d)$  код, який заданий над кінцевим полем  $GF(q)$  перевіркою  $(n-k) \times n$  матрицею  $H$ , за допомогою пристроїв кодування маскують невиродженою  $k \times k$  матрицею  $X$  з елементами із  $GF(q)$ , діагональною  $n \times n$  матрицею  $D$  з ненульовими на діагоналі елементами із  $GF(q)$ , переставною  $n \times n$  матрицею  $P$  з елементами із  $GF(q)$ . Для формування електронного цифрового підпису  $Y = (e, i)$  інформаційного повідомлення  $M$  за допомогою функції хешування  $h(x)$  обчислюють хеш-код  $h(M)$ , після чого послідовним збільшенням змінної-лічильника  $i$  обчислюють такий хеш-код  $h(h(M) \| i)$ , який відповідає синдромній послідовності  $s_X$  замаскованого  $(n, k, d)$  коду із перевіркою  $(n-k) \times n$  матрицею  $H_X = X \cdot H \cdot P \cdot D$ . Вектор помилок  $e$  обчислюють шляхом демаскування та алгебраїчного декодування послідовності  $s_X$ , для перевірки електронного цифрового підпису обчислюють хеш-код  $h(h(M) \| i)$  та порівнюють його із синдромною послідовністю  $s_X$ , яку обчислюють за матрицею  $H_X$ :  $(s'_X)^T = H_X \cdot e^T$ . При цьому проводять додаткову перевірку ваги Хеммінга вектора  $e$ , тобто підпис  $Y = (e, i)$  інформаційного повідомлення  $M$  вважають правильним, якщо виконується умова  $Y_n = (e, i) : H_X \cdot e^T = (h(h(M) \| i))^T, w(e) \leq t$ .

**UA 116152 U**



Запропонована корисна модель належить до галузі криптографічного захисту інформації за допомогою кодів і може бути використана в засобах несиметричного шифрування та електронного цифрового підпису у системах обробки інформації для розширення їх можливостей.

Відомий спосіб формування та перевірки електронного цифрового підпису із використанням алгебраїчних блокових кодів [1], який ґрунтується на тому, що лінійний алгебраїчний блоковий код за допомогою пристроїв кодування маскується невідродженими матрицями (які є секретним, приватним ключем), а для формування електронного цифрового підпису інформаційного повідомлення за допомогою функції хешування обчислюють хеш-код, який відповідає синдромній послідовності замаскованого коду, вектор помилок (як елемент підпису) обчислюють шляхом демаскування та алгебраїчного декодування синдромної послідовності. Для перевірки електронного цифрового підпису обчислюють хеш-код інформаційного повідомлення та порівнюють його із синдромною послідовністю, яку обчислюють за перевіркою матрицею замаскованого коду (яка є відкритим, публічним ключем).

Недоліком цього способу є можливість швидкої підробки підпису із використанням кодових слів замаскованого коду: якщо обрати довільне кодове слово та додати його до вектора помилок, тоді підроблений електронний цифровий підпис за результатом перевірки буде визначено як правильний.

Найбільш близьким до запропонованого технічним рішенням, обраним як прототип, є спосіб формування та перевірки електронного цифрового підпису із використанням алгебраїчних блокових кодів [2], який ґрунтується на тому, що лінійний алгебраїчний блоковий  $(n, k, d)$  код, який заданий над кінцевим полем  $GF(q)$  перевіркою  $(n - k) \times n$  матрицею  $H$ , за допомогою пристроїв кодування маскується невідродженою  $k \times k$  матрицею  $X$  з елементами із  $GF(q)$ , діагональною  $n \times n$  матрицею  $D$  з ненульовими на діагоналі елементами із  $GF(q)$ , переставною  $n \times n$  матрицею  $P$  з елементами із  $GF(q)$ , а для формування електронного цифрового підпису  $Y = (e, i)$  інформаційного повідомлення  $M$  за допомогою функції хешування  $h(x)$  обчислюють хеш-код  $h(M)$ , після чого послідовним збільшенням змінної-лічильника  $i$  обчислюють такий хеш-код  $h(h(M) \parallel i)$ , який відповідає синдромній послідовності  $s_X$  замаскованого  $(n, k, d)$  коду із перевіркою  $(n - k) \times n$  матрицею  $H_X = X \cdot H \cdot P \cdot D$ , вектор помилок  $e$  обчислюють шляхом демаскування та алгебраїчного декодування послідовності  $s_X$ . Де  $d$  - це мінімальне з відстаней Хеммінга для всіх пар кодових слів,  $t$  - це виправляюча здатність лінійного коду.

Для перевірки електронного цифрового підпису обчислюють хеш-код  $h(h(M) \parallel i)$  та порівнюють його із синдромною послідовністю  $s_X$ , яку обчислюють за матрицею  $H_X$ :

$$(s'_X)^T = H_X \cdot e^T,$$

тобто підпис  $Y = (e, i)$  інформаційного повідомлення  $M$  вважають правильним, якщо виконується рівність

$$Y_n = (e, i) : H_X \cdot e^T = (h(h(M) \parallel i))^T. \quad (1)$$

Матриці  $X$  і  $P$  використовують як секретний (приватний) ключ, а матрицю  $H_X$  - як відкритий (публічний) ключ.

Алгоритм формування електронного цифрового підпису подають у такій послідовності кроків [2].

Крок 1. Хешування відкритого тексту  $M$ , тобто обчислення хеш-коду  $h(M)$ . Присвоювання змінній  $i$  значення  $i = 1$ ;

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

Крок 3. Значення  $h(h(M) \parallel i)$  інтерпретується як синдромна послідовність  $s_X = (s_0, s_1, \dots, s_{n-k-1})$ , обчислена для деякого (довільного) кодового слова  $c = (c_0, c_1, \dots, c_{n-1})$  і вектора помилок  $e$ , тобто передбачається виконання рівності  $s_X^T = H_X \cdot e^T$  для відповідного відкритого ключа  $H_X = X \cdot H \cdot P$ ;

Крок 4. Обчислення вектора

$$s_X^{*T} = X^{-1} \cdot s_X^T,$$

який (як передбачається) являє собою синдром, обчислений за перевіркою матрицею  $H$  алгебраїчного  $(n, k, d)$  коду, тобто передбачається, що

$$s_X^{*T} = X^{-1} \cdot s_X^T = X^{-1} \cdot H_X \cdot e^T = H \cdot P \cdot e^T = H \cdot \bar{e}^T$$

і алгоритм швидкого (алгебраїчного) декодування дозволить знайти вектор  $\bar{e}^T = P \cdot e^T$ ;

5 Крок 5. Для синдромної послідовності  $s_X^*$  реалізується виконання швидкого (алгебраїчного) алгоритму декодування:

- якщо декодування досягло успіху - виводиться знайдений вектор помилок  $\bar{e}^T = P \cdot e^T$ , який відповідає вектору  $s_X^*$ ;

10 - якщо декодування не досягло успіху - видається повідомлення про неможливість знайти вектор помилок  $\bar{e}^T = P \cdot e^T$  для введенного вектора  $s_X^*$ . Далі виконується присвоєння змінної  $i$  значення  $i = i + 1$  і перехід на Крок 2;

Крок 6. Обчислення вектора

$$e^T = P^{-1} \cdot \bar{e}^T = P^{-1} \cdot P \cdot e^T;$$

Крок 7. Формування електронного цифрового підпису  $Y = (e, i)$  для відкритого тексту  $M$ .

15 Алгоритм перевірки електронного цифрового підпису подають у такій послідовності кроків [2].

Крок 1. Обчислення вектора

$$(s_X')^T = H_X \cdot e^T;$$

Крок 2. Обчислення вектора

20  $(s_X'')^T = h(h(M) \| i);$

Крок 3. Прийняття рішення про правильність чи неправильність електронного цифрового підпису:

- якщо  $s_X' = s_X''$ , тоді приймається рішення про правильність електронного цифрового підпису;

25 - якщо  $s_X' \neq s_X''$ , тоді приймається рішення про неправильність електронного цифрового підпису.

Недоліком цього способу є можливість швидкої підробки підпису  $Y = (e, i)$  із використанням кодових слів замаскованого  $(n, k, d)$  коду. Дійсно, якщо обрати довільне кодове слово  $c = (c_0, c_1, \dots, c_{n-1})$  використовуваного  $(n, k, d)$  коду з перевіркою матрицею  $H_X = X \cdot H \cdot P \cdot D$ , тоді очевидна рівність  $H_X \cdot c^T = 0$  призведе до можливості гарантовано підробити підпис  $Y_n = (e + c, i)$ , причому рівність (1) також буде виконуватися:

$$Y_n = (e + c, i) : H_X \cdot (e + c)^T = H_X \cdot e^T + H_X \cdot c^T = H_X \cdot e^T = (h(h(M) \| i))^T.$$

35 В основу корисної моделі поставлена задача створити спосіб формування та перевірки електронного цифрового підпису із використанням алгебраїчних блокових кодів, який, за рахунок додаткової перевірки ваги Хеммінга вектора помилок, дозволяє забезпечити захищеність від швидкої підробки підпису шляхом додавання до вектора помилок довільного кодового слова замаскованого  $(n, k, d)$  коду.

40 Поставлена задача вирішується наступним чином. У способі формування та перевірки електронного цифрового підпису із використанням алгебраїчних блокових кодів, який полягає в тому, що лінійний алгебраїчний блоковий  $(n, k, d)$  код, який заданий над кінцевим полем  $GF(q)$  перевіркою  $(n - k) \times n$  матрицею  $H$ , за допомогою пристроїв кодування маскують невиродженою  $k \times k$  матрицею  $X$  з елементами із  $GF(q)$ , діагональною  $n \times n$  матрицею  $D$  з ненульовими на діагоналі елементами із  $GF(q)$ , переставною  $n \times n$  матрицею  $P$  з елементами із  $GF(q)$ , а для формування електронного цифрового підпису  $Y = (e, i)$  інформаційного повідомлення  $M$  за допомогою функції хешування  $h(x)$  обчислюють хеш-код  $h(M)$ , після чого

45 послідовним збільшенням змінної-лічильника  $i$  обчислюють такий хеш-код  $h(h(M) \| i)$ , який відповідає синдромній послідовності  $s_X$  замаскованого  $(n, k, d)$  коду із перевіркою матрицею  $H_X = X \cdot H \cdot P \cdot D$ , вектор помилок  $e$  обчислюють шляхом демаскування та

алгебраїчного декодування послідовності  $s_X$ . Для перевірки електронного цифрового підпису обчислюють хеш-код  $h(h(M)||i)$  та порівнюють його із синдромною послідовністю  $s_X$ , яку обчислюють за матрицею  $H_X$ :

$$(s'_X)^T = H_X \cdot e^T.$$

- 5 Згідно з корисною моделлю, проводять додаткову перевірку ваги Хеммінга вектора  $e$ , тобто підпис  $Y = (e, i)$  інформаційного повідомлення  $M$  вважають правильним, якщо виконується умова

$$Y_n = (e, i) : H_X \cdot e^T = (h(h(M)||i))^T, w(e) \leq t.$$

- 10 Запропонований спосіб формування та перевірки електронного цифрового підпису із використанням алгебраїчних блокових кодів ґрунтується на тому, що лінійний алгебраїчний блоковий  $(n, k, d)$  код, який заданий над кінцевим полем  $GF(q)$  перевіркою  $(n - k) \times n$  матрицею  $H$ , за допомогою пристроїв кодування маскують невиродженою  $k \times k$  матрицею  $X$  з елементами із  $GF(q)$ , діагональною  $n \times n$  матрицею  $D$  з ненульовими на діагоналі елементами із  $GF(q)$ , переставною  $n \times n$  матрицею  $P$  з елементами із  $GF(q)$  а для формування
- 15 електронного цифрового підпису  $Y = (e, i)$  інформаційного повідомлення  $M$  за допомогою функції хешування  $h(x)$  обчислюють хеш-код  $h(M)$ , після чого послідовним збільшенням змінної-лічильника  $i$  обчислюють такий хеш-код  $h(h(M)||i)$ , який відповідає синдромній послідовності  $s_X$  замаскованого  $(n, k, d)$  коду із перевіркою  $(n - k) \times n$  матрицею  $H_X = X \cdot H \cdot P \cdot D$ , вектор помилок  $e$  обчислюють шляхом демаскування та алгебраїчного
- 20 декодування послідовності  $s_X$ . Для перевірки електронного цифрового підпису обчислюють хеш-код  $h(h(M)||i)$  та порівнюють його із синдромною послідовністю  $s_X$ , яку обчислюють за матрицею  $H_X$ :

$$(s'_X)^T = H_X \cdot e^T,$$

- із додатковою перевіркою ваги Хеммінга вектора  $e$ , тобто підпис  $Y = (e, i)$  інформаційного
- 25 повідомлення  $M$  вважають правильним, якщо виконується умова

$$Y_n = (e, i) : H_X \cdot e^T = (h(h(M)||i))^T, w(e) \leq t. \quad (2)$$

Матриці  $X$  і  $P$  використовують як секретний (приватний) ключ, а матрицю  $H_X$  - як відкритий (публічний) ключ.

- Алгоритм формування електронного цифрового підпису подають у такій послідовності
- 30 кроків.

Крок 1. Хешування відкритого тексту  $M$ , тобто обчислення хеш-коду  $h(M)$ . Присвоювання змінній  $i$  значення  $i = 1$ ;

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

- 35 Крок 3. Значення  $h(h(M)||i)$  інтерпретується як синдромна послідовність  $s_X = (s_0, s_1, \dots, s_{n-k-1})$ , обчислена для деякого (довільного) кодового слова  $c = (c_0, c_1, \dots, c_{n-1})$  і вектора помилок  $e = (e_0, e_1, \dots, e_{n-1})$ , тобто передбачається виконання рівності  $s_X^T = H_X \cdot e^T$  для відповідного відкритого ключа  $H_X = X \cdot H \cdot P$ ;

Крок 4. Обчислення вектора

$$s_X^{*T} = X^{-1} \cdot s_X^T,$$

який (як передбачається) являє собою синдром, обчислений за перевіркою матрицею  $H$  алгебраїчного  $(n, k, d)$  коду, тобто передбачається, що

$$s_X^{*T} = X^{-1} \cdot s_X^T = X^{-1} \cdot H_X \cdot e^T = H \cdot P \cdot e^T = H \cdot \bar{e}^T$$

і алгоритм швидкого (алгебраїчного) декодування дозволить знайти вектор  $\bar{e}^T = P \cdot e^T$ ;

- 45 Крок 5. Для синдромної послідовності  $s_X^*$  реалізується виконання швидкого (алгебраїчного) алгоритму декодування:

- якщо декодування досягло успіху - виводиться знайдений вектор помилок  $\bar{e}^T = P \cdot e^T$ , який відповідає вектору  $s_X^*$ ;

- якщо декодування не досягло успіху - видається повідомлення про неможливість знайти вектор помилок  $\bar{e}^T = P \cdot e^T$  для введеного вектору  $s_X^*$ . Далі виконується присвоєння змінної  $i$  значення  $i = i + 1$  і перехід на Крок 2;

5      Крок 6. Обчислення вектора

$$e^T = P^{-1} \cdot \bar{e}^T = P^{-1} \cdot P \cdot e^T;$$

Крок 7. Формування електронного цифрового підпису  $Y = (e, i)$  для відкритого тексту  $M$ .

Алгоритм перевірки електронного цифрового підпису подають у такій послідовності кроків.

10      Крок 1. Обчислення вектора

$$(s'_X)^T = H_X \cdot e^T;$$

Крок 2. Обчислення вектора

$$(s''_X)^T = h(h(M)||i);$$

15      Крок 3. Прийняття рішення про правильність чи неправильність електронного цифрового підпису:

- якщо  $s'_X = s''_X$  та  $w(e) \leq t$ , тоді приймається рішення про правильність електронного цифрового підпису;

- якщо  $s'_X \neq s''_X$  та (або)  $w(e) > t$ , тоді приймається рішення про неправильність електронного цифрового підпису.

20      В порівнянні із способом-прототипом швидка підробка підпису  $Y = (e, i)$  шляхом додавання до вектора помилок  $e = (e_0, e_1, \dots, e_{n-1})$  довільного кодового слова  $c = (c_0, c_1, \dots, c_{n-1})$  використовуюваного  $(n, k, d)$  коду з перевіркою  $(n-k) \times n$  матрицею  $H_X = X \cdot H \cdot P \cdot D$  буде гарантовано виявлена. Дійсно, вага Хеммінга кодового слова задовольняє умові  $w(c) \geq d = 2t + 1$ , тобто для підробленого підпису  $Y_n = (e + c, i)$  буде завжди виконуватися умова

25       $w(e + c) > t$ . Саме цей випадок унеможливується на Кроці 3 алгоритму перевірки підпису.

Таким чином, досягається технічний результат, який може бути отриманий при здійсненні запропонованого способу, а саме вдається забезпечити захищеність від швидкої підробки підпису із використанням кодових слів замаскованого  $(n, k, d)$  коду.

Джерела інформації:

30      1. Courtois, N., Finiasz, M., and N.Sendrier: How to achieve a McEliece-based digital signature scheme. In Advances in Cryptology-ASIACRYPT 2001, volume 2248, pages 157-174

2. Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik. Post-Quantum Cryptography. - 2009, Springer-Verlag, Berlin-Heidelberg. - 245 p.

### 35      ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб формування та перевірки електронного цифрового підпису із використанням алгебраїчних блокових кодів, який полягає в тому, що лінійний алгебраїчний блоковий  $(n, k, d)$  код, який заданий над кінцевим полем  $GF(q)$  перевіркою  $(n-k) \times n$  матрицею  $H$ , за допомогою пристроїв кодування маскують невиродженою  $k \times k$  матрицею  $X$  з елементами із  $GF(q)$ , діагональною  $n \times n$  матрицею  $D$  з ненульовими на діагоналі елементами із  $GF(q)$ , переставною  $n \times n$  матрицею  $P$  з елементами із  $GF(q)$ , а для формування електронного цифрового підпису  $Y = (e, i)$  інформаційного повідомлення  $M$  за допомогою функції хешування  $h(x)$  обчислюють хеш-код  $h(M)$ , після чого послідовним збільшенням змінної-лічильника  $i$

45      обчислюють такий хеш-код  $h(h(M)||i)$ , який відповідає синдромній послідовності  $s_X$  замаскованого  $(n, k, d)$  коду із перевіркою  $(n-k) \times n$  матрицею  $H_X = X \cdot H \cdot P \cdot D$ , вектор помилок  $e$  обчислюють шляхом демаскування та алгебраїчного декодування послідовності  $s_X$ , для перевірки електронного цифрового підпису обчислюють хеш-код  $h(h(M)||i)$  та порівнюють його із синдромною послідовністю  $s_X$ , яку обчислюють за матрицею  $H_X$ :

50       $(s'_X)^T = H_X \cdot e^T,$

який **відрізняється** тим, що проводять додаткову перевірку ваги Хеммінга вектора  $e$ , тобто підпис  $Y = (e, i)$  інформаційного повідомлення  $M$  вважають правильним, якщо виконується умова

$$Y_n = (e, i) : H_X \cdot e^T = (h(h(M) \| i))^T, w(e) \leq t,$$

- 5 де  $k$  та  $n$  - цілі позитивні числа с  $k < n$ ,  
 $d$  - це мінімальне з відстаней Хеммінга для всіх пар кодових слів,  
 $i$  - це ціле число,  $i \geq 1$ ,  
 $t$  - це виправляюча здатність лінійного коду,  
 $q$  - це кількість елементів поля  $GF(q)$ .

10

---

Комп'ютерна верстка Г. Паяльніков

---

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

---

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601