



УКРАЇНА

(19) UA (11) 55211 (13) U  
(51) МПК (2009)  
H04L 9/06

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під  
відповідальність  
власника  
патенту

(54) КОНВЕЕРНИЙ КРИПТОГРАФІЧНИЙ ОБЧИСЛЮВАЧ

1

2

(21) u201006041

(22) 19.05.2010

(24) 10.12.2010

(46) 10.12.2010, Бюл. № 23, 2010 р.

(72) КОРЧЕНКО ОЛЕКСАНДР ГРИГОРОВИЧ, ПАЦІРА ЄВГЕНІЯ ВІКТОРІВНА, ПАНАСЮК АНДРІЙ ЛЕОНІДОВИЧ, ГНАТЮК СЕРГІЙ ОЛЕКСАНДРОВИЧ, КІНЗЕРЯВИЙ ВАСИЛЬ МИКОЛАЙОВИЧ

(73) НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

(57) 1. Конвеєрний криптографічний обчислювач, що містить модуль початкової обробки,  $6+2n$

( $n=2,4$ ) модулів шифрування та модуль формування результату, який відрізняється тим, що додатково введено синхронізуючу шину (СШ), 128-бітну вхідну шину даних,  $(64n)$ -бітну вхідну шину ключа та 128-бітну вихідну шину даних, причому вхідна шина ключа підключена до першого входу модуля початкової обробки, другий вхід якого з'єднаний з вхідною шиною даних, а перший вихід підключений до першого входу першого модуля шифрування, вихід  $i$ -го ( $i=\overline{1,5+2n}$ ) модуля шифрування з'єднаний з першим входом  $(i+1)$ -го ( $i=\overline{1,5+2n}$ ) модуля шифрування, другий вхід  $i$ -го ( $i=\overline{1,6+2n}$ ) модуля шифрування відповідно з'єднаний з  $(i+1)$ -им ( $i=\overline{1,6+2n}$ ) виходом модуля початкової обробки, а третій вхід  $i$ -го ( $i=\overline{1,6+2n}$ ) модуля шифрування підключений до синхронізуючої шини, при цьому вихід  $(6+2n)$ -го модуля шифрування з'єднаний з модулем формування результату, вихід якого з'єднаний з вихідною шиною даних.

2. Конвеєрний криптографічний обчислювач за п. 1, який відрізняється тим, що модуль початкової обробки містить блок початкової обробки ключа, блок початкової обробки даних, блок додавання за модулем 2 ( $M2$ ), причому другий вхід модуля початкової обробки з'єднаний з входом блока початкової обробки даних, вихід якого підключений до другого входу блока  $M2$ , вихід якого з'єднаний з першим виходом модуля початкової обробки, а перший вхід підключений до першого виходу блока початкової обробки ключа,  $(i+1)$ -ий ( $i=\overline{1,6+2n}$ ) вихід якого відповідно підключений до  $(i+1)$ -го

( $i=\overline{1,6+2n}$ ) виходу модуля початкової обробки, а вхід з'єднаний з першим входом модуля початкової обробки.

3. Конвеєрний криптографічний обчислювач за п.

1, який відрізняється тим, що  $i$ -ий ( $i=\overline{1,5+2n}$ ) модуль шифрування містить інвертувальний блок функціонального перетворення, інвертувальний блок нелінійного перетворення, блок  $M2$ , інвертувальний блок лінійного перетворення та регістр пам'яті, причому перший вхід модуля шифрування підключений до входу інвертувального блока функціонального перетворення, вихід якого з'єднаний з входом інвертувального блока нелінійного перетворення, вихід якого з'єднаний з другим входом блока  $M2$ , до першого входу якого підключений другий вхід модуля шифрування, а вихід підключений до входу блока лінійного перетворення, вихід якого з'єднаний з першим входом регістра пам'яті, другий вхід якого підключений до третього входу модуля шифрування, а вихід підключений до виходу модуля шифрування.

4. Конвеєрний криптографічний обчислювач за п. 1, який відрізняється тим, що  $(6+2n)$ -ий модуль шифрування містить інвертувальний блок функціонального перетворення, інвертувальний блок нелінійного перетворення, блок  $M2$  та регістр пам'яті, причому перший вхід модуля шифрування підключений до входу інвертувального блока функціонального перетворення, вихід якого з'єднаний з входом інвертувального блока нелінійного перетворення, вихід якого з'єднаний з другим входом блока  $M2$ , до першого входу якого підключений другий вхід модуля шифрування, а вихід підключений до першого входу регістра пам'яті, другий вхід якого з'єднаний з третім входом модуля шифрування, а вихід підключений до виходу модуля шифрування.

5. Конвеєрний криптографічний обчислювач за п. 1, який відрізняється тим, що модуль формування результату містить блок кінцевої обробки даних, вхід і вихід якого відповідно з'єднані з входом і виходом модуля формування результату.

UA (11) 55211 (13) U

Корисна модель належить до галузі криптографічного захисту інформації і може бути використана в засобах шифрування у системах обробки інформації для розширення їх можливостей.

Відомий спосіб криптографічного перетворення [1], який ґрунтується на тому, що інформаційну послідовність подають у вигляді 64-бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: перестановки (permutation) - за допомогою блоків перестановок (P-блоків); підстановки (substitution) - за допомогою блоків підстановок (S-блоків); функціональних операцій циклічного зсуву і додавання за модулем 2 - за допомогою відповідних блоків. Ітеративна обробка полягає у багатократному виконанні однакових груп перетворень, що забезпечують необхідні умови стійкості криптографічного перетворення: розсіювання (за допомогою P-блоків) та перемішування (за допомогою S-блоків) інформаційних даних.

Найбільш близьким, до запропонованого технічним рішенням, обраним як прототип, є криптографічний обчислювач для захисту інформації [2], відображений на систолічній конвеєрній структурі, який базується на способі криптографічного перетворення [1] та містить модуль початкової обробки, 16 модулів шифрування, модуль формування результату, дві 64-бітові шини входу, розряди яких утворюють масив, упорядкований відповідно до вихідної матриці, 64-бітову шину виходу і дворозрядну шину керування, через перший розряд якої надходить стробований сигнал запису результату

$i$ -ї ( $i = \overline{1, 16}$ ) ітерації шифрування чи дешифрування (Ш/Д), другий - визначає режим роботи систолічного криптографічного обчислювача шифрування чи дешифрування. Вхідні шини підключені до входів модуля початкової обробки, який з'єднаний з пер-

шим модулем шифрування, вихід  $z$ -го ( $i = \overline{1, 15}$ ) модуля шифрування з'єднаний з входом  $(i+1)$ -го

( $i = \overline{1, 15}$ ) модуля шифрування, шістнадцятий модуль шифрування з'єднаний з модулем формування результату, вихід якого підключений до вихідної шини.

Недоліком даного криптографічного обчислювача є не здатність алгоритму (покладеному в його основі) забезпечити достатню криптостійкість та високу швидкість обробки даних для використання в сучасних системах реального часу.

В основу корисної моделі поставлена задача забезпечення криптостійкості та швидкої криптографічної обробки в системах реального часу, особливо при обробці великих об'ємів даних.

Технічний результат, який може бути отриманий при створенні корисної моделі, полягає у забезпеченні достатньої криптостійкості та високої швидкості криптографічної обробки в системах реального часу.

Сутність запропонованої корисної моделі полягає в тому, що поставлена задача вирішується

за рахунок побудови конвеєрного криптографічного обчислювача, який базується на сучасному криптопостійкому алгоритмі дешифрування [3].

Використання відомого способу дешифрування [3] дає змогу значно збільшити криптостійкість, а його відображення на конвеєрну структуру у сукупності з використанням специфічних етапів криптографічної обробки, спрощенням етапів циклічної обробки та зменшенням кількості циклічних повторень вищезгаданого способу дешифрування дає змогу підвищити швидкість корисної моделі. У сукупності вищеперераховані ознаки роблять можлигим досягнення даного технічного результату.

На Фіг.1 зображена структурна схема конвеєрного криптографічного обчислювача.

Конвеєрний криптографічний обчислювач містить синхронізуючу шину (СШ), 128-бітну вхідну

шину даних,  $(64n)$ -бітну ( $n = \overline{2, 4}$ ) вхідну шину ключа та 128-бітну вихідну шину даних, модуль початкової обробки (МПО),  $6+2n$  модулів шифрування (МШ) та модуль формування результату (МФР). Модуль МПО містить блок початкової обробки ключа (БПОК), блок початкової обробки даних (БПОД), блок додавання за модулем 2 (М2).  $i$ -ий

( $i = \overline{1, 5+2n}$ ) МШ містить інвертний блок нелінійного перетворення (ІБНП), інвертний блок функціонального перетворення (ІБФП), інвертний блок лінійного перетворення (ІБЛП), блок М2 та регістр пам'яті (RG).  $(6+2n)$ -ий МШ містить ІБНП, ІБФП, блок М2 та RG. Модуль МФР містить блок кінцевої обробки даних (БКОД).

У загальному вигляді конвеєрний криптографічний обчислювач працює наступним чином. Перед початком обчислювального процесу  $(64n)$ -бітний

( $n = \overline{2, 4}$ ) ключ подають на МПО, де в БПОК відповідно генерується  $6+2n$  раундових ключів для кожного з раундів шифрування, які разом з ключем записуються у зворотному порядку до регістрів ключів, з виходу яких вони поступають на виходи МПО. Зашифровані дані у вигляді 128-бітних блоків даних (представлених у вигляді матриці) через вхідну шину даних поступають паралельним кодом у МПО. Після обробки в МПО блоки даних посту-

пають потактно до  $i$ -го ( $i = \overline{1, 6+2n}$ ) МШ, де спочатку у ІБФП відбувається циклічний зсув вправо всіх рядків блока даних, за виключенням нульового. Після чого, вони піддаються нелінійному перетворенню в ІБНП, а саме табличній заміні кожного байту блока даних. Після чого блок даних поступає на другий вхід блока М2, на перший вхід якого передається відповідний раундовий ключ з  $(i+1)$ -го

( $i = \overline{1, 6+2n}$ ) виходу МПО. Після цього, у ІБЛП виконується множення кожного стовпчика блока даних, який розглядається як поліном в кінцевому полі  $GF(2^8)$ , на фіксований поліном  $\alpha^{-1}(x) = Bx^3 + Dx^2 + 9x + E$ , множення відбувається за модулем  $x^4 + 1$ , далі за синхросигналом результат

заноситься в регістр пам'яті, з виходу якого дані поступають до виходу МШ. У  $(6+2n)$ -му МШ виключено ІБЛП, а з його виходу дані передаються до МФР, де оброблюються в БКОД, з виходу МФР шифровані дані поступає на вихідну шину даних.

Джерела інформації:

1. National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard." Oct. 1999. Available at <http://csrc.nist.gov/publications/fips>.

2. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. - К.: «МК-Пресс», 2006. - с. 207-214.

3. National Institute of Standards and Technology. "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at <http://csrc.nist.gov/publications/fips>.

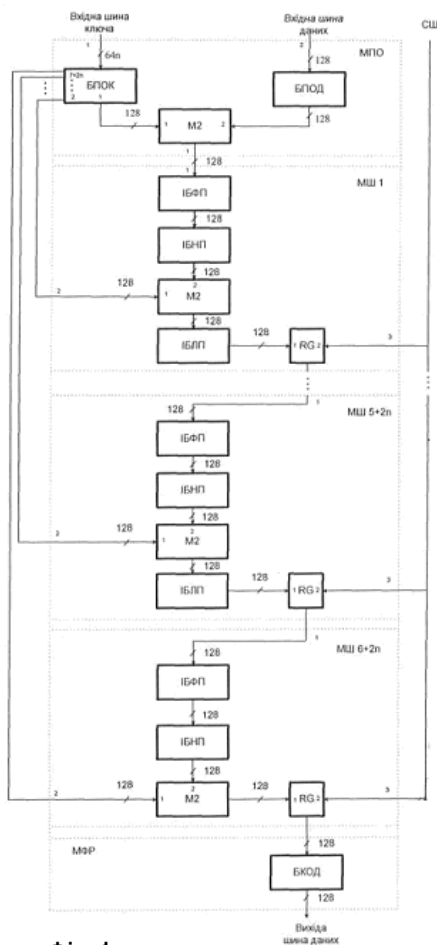


Fig 1