



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA**

(11) **67691**

(13) **U**

(51) МПК

H04L 9/06 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2010 06046**

(22) Дата подання заявки: **19.05.2010**

(24) Дата, з якої є чинними
права на корисну
модель: **12.03.2012**

(46) Публікація відомостей
про видачу патенту: **12.03.2012, Бюл.№ 5**

(72) Винахідник(и):

**Корченко Олександр Григорович (UA),
Паціра Євгенія Вікторівна (UA),
Малофєєв Олександр Вікторович (UA),
Гнатюк Сергій Олександрович (UA),
Кінзерявий Василь Миколайович (UA)**

(73) Власник(и):

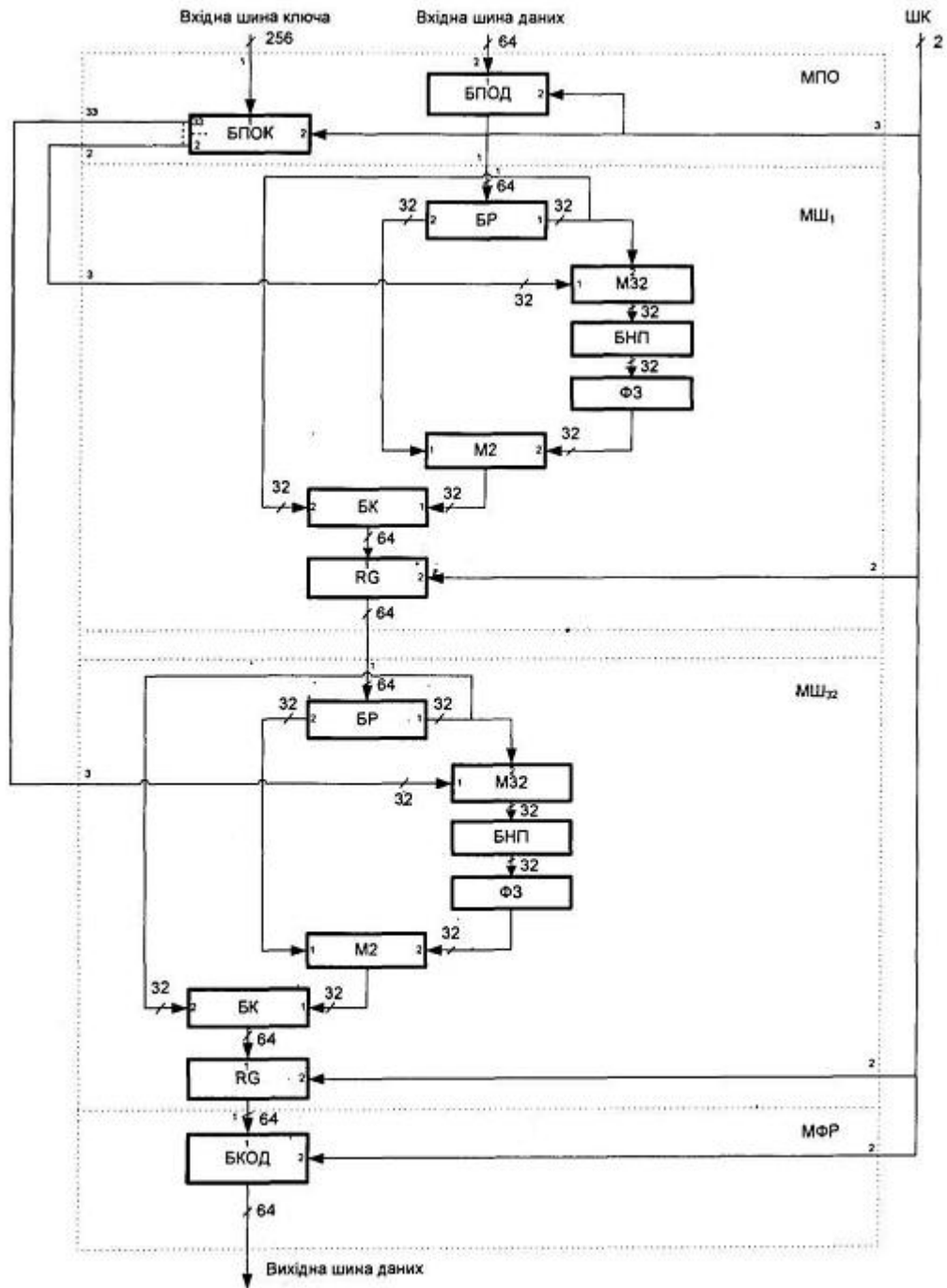
**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ
УНІВЕРСИТЕТ,
пр. Комарова, 1, м. Київ, 03680 (UA)**

(54) КОНВЕЄРНИЙ КРИПТОГРАФІЧНИЙ ОБЧИСЛЮВАЧ

(57) Реферат:

Конвеєрний криптографічний обчислювач містить 64-бітну вхідну шину даних, шину керування, модуль початкової обробки даних, 16 модулів шифрування, модуль формування результату та 64-бітну вихідну шину даних. Додатково містить 16 модулів шифрування та 256-бітну вхідну шину ключа.

UA 67691 U



Фиг. 1

Корисна модель належить до галузі криптографічного захисту інформації і може бути використана в засобах шифрування, в 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 за допомогою примітивних криптографічних перетворень: перестановок (за допомогою блоків перестановок - Р-блоків); підстановок (за допомогою блоків підстановок - S-блоків); функціональних операцій циклічного зсуву і додавання за модулем 2 (за допомогою відповідних блоків). Ітеративна обробка полягає в багатократному виконанні однакових груп перетворень, що забезпечують необхідні умови стійкості криптографічного перетворення: розсіювання (за допомогою Р-блоків) та перемішування (за допомогою S-блоків) інформаційних даних.

Найбільш близьким до запропонованого технічним рішенням, вибраним 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-бітні шини входу, розряди яких утворюють масив, упорядкований відповідно до вихідної матриці, 64-бітну 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 першим модулем шифрування, вихід i -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 систолічного криптографічного обчислювача є нездатність алгоритма, (покладеного в його основу), забезпечити достатню криптостійкість і високу швидкість обробки даних для використання в сучасних системах реального часу.

В основу корисної моделі поставлена задача забезпечення криптостійкого та швидкого шифрування в системах реального часу, особливо при обробці великих об'ємів даних.

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

Поставлена задача вирішується за рахунок побудови конвеєрного криптографічного обчислювача, який базується на сучасному криптостійкому алгоритмі шифрування [3] при побудові в конвеєрного криптографічного обчислювача. Для цього в конвеєрний криптографічний обчислювач, який містить 64-бітну вхідну шину даних, шину керування, модуль початкової обробки даних, 16 модулів шифрування, модуль формування результату та 64-бітну вихідну шину даних, причому 64-бітна вхідна шина даних підключена до другого 64-бітного входу модуля початкової обробки, до першого 64-бітного входу якого підключений перший 64-бітний вхід першого модуля шифрування, 64-бітний вихід i -го ($i = \overline{1,15}$) модуля шифрування відповідно з'єднаний з першим 64-бітним входом $(i+1)$ -го ($i = \overline{1,15}$) модуля шифрування, шина керування підключена до другого входу i -го ($i = \overline{1,16}$) модуля шифрування, третього входу модуля початкової обробки та другого входу модуля формування результату, до виходу якого підключена 64-бітна вихідна шина даних, згідно з корисною моделлю, додатково введено 16 модулів шифрування та 256-бітну вхідну шину ключа, причому 64-бітний вихід i -го ($i = \overline{1,31}$) модуля шифрування відповідно підключений до першого 64-бітного входу $(i+1)$ -го ($i = \overline{1,31}$) модуля шифрування, 64-бітний вихід 32-го модуля шифрування підключений до першого 64-бітного входу модуля формування результату, другий вхід i -го ($i = \overline{17,32}$) модуля шифрування з'єднаний з шиною керування, а до третього 32-бітного входу i -го ($i = \overline{1,32}$) модуля шифрування відповідно підключений $(i+1)$ -й ($i = \overline{1,32}$) 32-бітний вихід модуля початкової обробки, перший 256-бітний вхід якого підключений до 256-бітної вхідної шини ключа. Також була виконана модифікація модуля початкової обробки, i -го ($i = \overline{1,32}$) модуля шифрування та модуля формування результату.

Використання відомого способу криптографічного перетворення [3] дає змогу значно збільшити криптостійкість, а його відображення на конвеєрну структуру, в сукупності з використанням специфічних етапів шифрування, спрощенням етапів циклічної обробки

вищезгаданого способу криптографічного перетворення, дає змогу підвищити швидкодію корисної моделі. У сукупності вищеперераховані ознаки роблять можливим досягнення даного технічного результату.

На кресленні зображена структурна схема конвеєрного криптографічного обчислювача.

5 Конвеєрний криптографічний обчислювач містить шину керування (ПІК), 256-бітну вхідну шину ключа, 64-бітну вхідну шину даних, 64-бітну вихідну шину даних, модуль початкової обробки (МПО), 32 модулі шифрування (МШ) та модуль формування результату (МФР). Модуль МПО містить блок початкової обробки ключа (БПОК) та блок початкової обробки даних (БПОД).
 10 i -й ($i = \overline{1,32}$) МШ містить блок розділення (БР), блок складання за модулем 32 (М32), блок нелінійних перетворень (БНП), формувач зсувів (ФЗ), блок складання за модулем 2 (М2), блок конкатенації (БК) та регістр пам'яті (RG). МФР містить блок кінцевої обробки даних (БКОД).

У загальному вигляді конвеєрний криптографічний обчислювач працює наступним чином. Перед початком обчислювального процесу ключ подають в БПОК модуля МПО, де формуються 32 раундових ключі (в залежності від сигналу ШК) для кожного з раундів шифрування, які
 15 записуються в регістри ключів, з виходу яких вони надходять на виходи МПО. Вхідні дані у вигляді 64-бітних блоків, через вхідну шину даних, надходять паралельним кодом у МПО, де оброблюються в БПОД (в залежності від ШК). Після обробки в МПО блоки даних надходять потактно до i -го ($i = \overline{1,32}$) МШ, де вони в БР спочатку розбиваються на молодші 32 біти ($\overline{1,32}$) та старші 32 біти ($\overline{33,64}$). Молодші біти з першого виходу БР передаються далі до М32, де вони
 20 складаються за модулем 32 із раундовим ключем з $(i+1)$ -го ($i = \overline{1,32}$) виходу МПО, а результат подається в БНП, де відбувається таблична заміна кожного біта даних. З БНП дані подаються до ФЗ, де вони піддаються циклічному зсуву. Після чого результат складають за модулем 2 в блоці М2 зі старшими бітами, що надходять з другого виходу БР. Далі одержані дані разом з молодшими бітами з першого виходу БР подають в БК, де здійснюють їхню конкатенацію, а
 25 результат за синхросигналом заноситься в RG. З виходу 32-го модуля МШ шифрований текст поступає до МФР, де оброблюється в БКОД (в залежності від ШК), з виходу МФР шифрований текст надходить на вихідну шину даних.

Джерела інформації:

1. National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard." Oct.
 30 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. ДСТУ ГОСТ 28147:2009 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

35

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

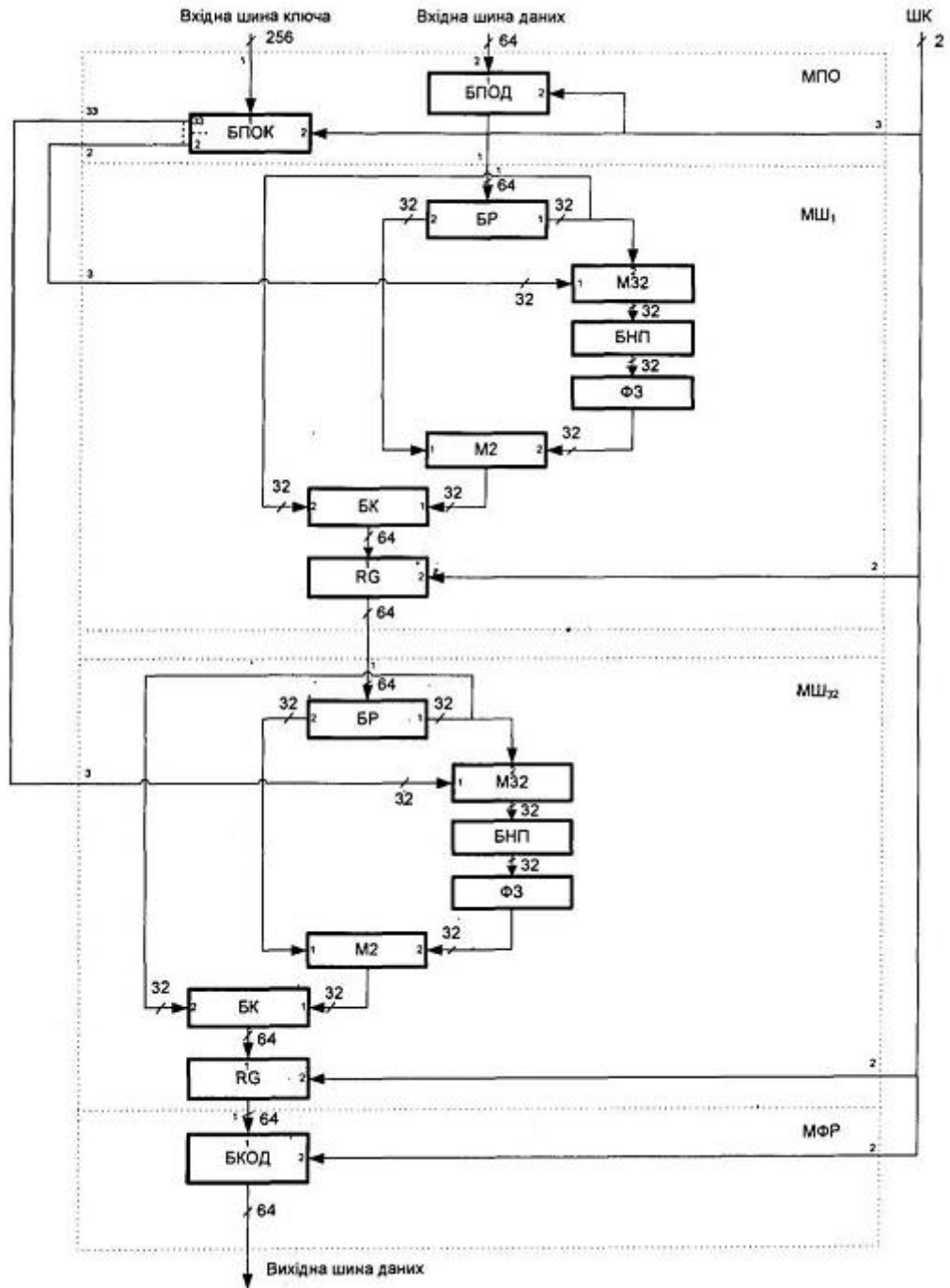
1. Конвеєрний криптографічний обчислювач містить 64-бітну вхідну шину даних, шину керування, модуль початкової обробки даних, 16 модулів шифрування, модуль формування
 40 результату та 64-бітну вихідну шину даних, причому 64-бітна вхідна шина даних підключена до другого 64-бітного входу модуля початкової обробки, до першого 64-бітного виходу якого підключений перший 64-бітний вхід першого модуля шифрування, 64-бітний вихід i -го ($i = \overline{1,15}$) модуля шифрування відповідно з'єднаний з першим 64-бітним входом $(i+1)$ -го ($i = \overline{1,15}$) модуля шифрування, шина керування підключена до другого входу i -го ($i = \overline{1,16}$) модуля шифрування,
 45 третього входу модуля початкової обробки та другого входу модуля формування результату, до виходу якого підключена 64-бітна вихідна шина даних, який **відрізняється тим**, що додатково введено 16 модулів шифрування та 256-бітну вхідну шину ключа, причому 64-бітний вихід i -го ($i = \overline{1,31}$) модуля шифрування відповідно підключений до першого 64-бітного входу $(i+1)$ -го ($i = \overline{1,31}$) модуля шифрування, 64-бітний вихід 32-го модуля шифрування підключений до
 50 першого 64-бітного входу модуля формування результату, другий вхід i -го ($i = \overline{17,32}$) модуля шифрування з'єднаний з шиною керування, а до третього 32-бітного входу i -го ($i = \overline{1,32}$) модуля шифрування відповідно підключений $(i+1)$ -й ($i = \overline{1,32}$) 32-бітний вихід модуля початкової обробки, перший 256-бітний вхід якого підключений до 256-бітної вхідної шини ключа.

2. Конвеєрний криптографічний обчислювач за п. 1, який **відрізняється тим**, що модуль
 55 початкової обробки містить блок початкової обробки даних та блок початкової обробки ключа, причому перший 256-бітний вхід модуля початкової обробки підключений до першого 256-

бітного входу блока початкової обробки ключа, i -й $(1,32)$ 52-бітний вихід якого відповідно підключений до $(i+1)$ -го $(1,32)$ 32-бітного виходу модуля початкової обробки, а третій вхід модуля початкової обробки з'єднаний з другим входом блока початкової обробки ключа та з другим входом блока початкової обробки даних, до першого 64-бітного входу якого підключений
 5 другий 64-бітний вхід модуля початкової обробки, а 64-бітний вихід з'єднаний з першим 64-бітним виходом модуля початкової обробки.

3. Конвеєрний криптографічний обчислювач за п. 1, який **відрізняється тим**, що i -й $(1,32)$ модуль шифрування містить блок розділення, блок конкатенації, блок складання за модулем 32, блок нелінійних перетворень, формувач-зсувів, блок складання за модулем 2, регістр пам'яті,
 10 причому перший 64-бітний вхід модуля шифрування підключений до 64-бітного входу блока розділення, перший 32-бітний вихід якого з'єднаний з другим 32-бітним входом блока складання за модулем 32, до першого 32-бітного входу якого підключений третій 32-бітний вхід модуля шифрування, а 32-бітний вихід з'єднаний з 32-бітним входом блока нелінійних перетворень, 32-бітний вихід якого підключений до 32-бітного входу формувача зсувів, до 32-бітного виходу
 15 якого підключений другий 32-бітний вхід блока складання за модулем 2, до першого 32-бітного входу якого підключений, другий 32-бітний вихід блока розділення, а 32-бітний вихід з'єднаний з першим 32-бітним входом блока конкатенації, до другого 32-бітного входу якого підключений перший 32-бітний вихід блока розділення, а 64-бітний вихід підключений до першого 64-бітного входу регістра пам'яті, другий вхід якого з'єднаний з другим входом модуля шифрування, а до
 20 64-бітного виходу підключений 64-бітний вихід модуля шифрування.

4. Конвеєрний криптографічний обчислювач за п. 1, який **відрізняється тим**, що модуль формування результату містить блок кінцевої обробки даних, причому перший 64-бітний вхід модуля формування результату підключений до першого 64-бітного входу блока кінцевої обробки даних, другий вхід якого з'єднаний з другим входом модуля формування результату, а
 25 64-бітний вихід підключений до 64-бітної шини вихідних даних.



Комп'ютерна верстка А. Крижанівський

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

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