УКРАЇНА

(19) UA (11) 61270 (13) U

(51) МПК
H04L 9/06 (2006.01)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) ПРИСТРІЙ ДЛЯ ШИФРУВАННЯ ДАНИХ В РЕЖИМІ ЗЧЕПЛЕННЯ БЛОКІВ ДАНИХ

(21) u201100465
(22) 17.01.2011
(24) 11.07.2011
(46) 11.07.2011, Бюл.№ 13, 2011 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Пристрій для шифрування даних в режимі зчеплення блоків даних, що містить оперативно запам'ятовуючий пристрій, сполучений із першим регістром даних, першим суматором за модулем два, що сполучений із криптографічним процесором, сполучений із другим суматором за модулем два, сполучений із оперативно запам'ятовуючим пристроєм, перший пристрій логічного множення, сполучений із першим суматором за модулем два, другий пристрій логічного множення, сполучений із другим суматором за модулем два, другий регістр даних, який **відрізняється** тим, що додатково введено комутатор, пристрій додавання за модулем 2^n, третій суматор за модулем два, третій регістр даних, генератор псевдовипадкових послідовностей бітів, при цьому перший регістр даних сполучений із комутатором, сполучений із пристроєм додавання за модулем 2^n, сполучений із третім регістром даних, першим і другим пристроями логічного множення, третій регістр даних сполучений із пристроєм додавання за модулем 2^n, другий суматор за модулем два сполучений із другим регістром даних, сполучений із комутатором, генератор псевдовипадкових послідовностей бітів сполучений із третім суматором за модулем два, сполучений із керуючим входом комутатора.

1

Корисна модель відноситься до галузі криптографічного захисту інформації і може бути використана в засобах шифрування та у системах обробки інформації під час передачі та зберігання даних.

Відомий пристрій шифрування даних в режимі зчеплення блоків зашифрованих текстів, який містить вхідний буфер, сполучений із регістром вхідних даних, сполучений із суматором за модулем два, сполучений із криптографічним процесором, сполучений із регістром вихідних даних, сполучений із суматором за модулем два, комутатор, сполучений із буфером вихідних даних, регістр вектора ініціалізації, сполучений із суматором за модулем два, регістр маски, регістр лічильника, сполучені із буфером вхідних даних, буфером вихідних даних, схеми керування зчитуванням даних з вхідного буфера та записом у вихідний буфер [Патент США № 4907275, МІЖ H04L9/02, 6.03.1990 р.].

Недоліками аналогу є те, що режим зчеплення блоків зашифрованого тексту є слабким до атак "дня народження" і "зустрічі по середині", за рахунок яких порушується цілісність повідомлення і не забезпечується достатній рівень криптографічної стійкості.

2

Найбільш близьким за сукупністю ознак до запропонованого є пристрій для зашифрування/розшифрування даних в режимі зчеплення блоків зашифрованих текстів, що містить оперативно запам'ятовуючий пристрій (ОЗП), сполучений із першим регістром даних, першим суматором за модулем два, що сполучений з криптографічним процесором (КП), сполучений із першим пристроєм логічного множення, другим суматором за модулем два, сполучений із (ОЗП, перший регістр даних сполучено з другим регістром даних, сполучений із другим пристроєм логічного множення, сполучений із другим суматором за модулем два, перший пристрій логічного множення, сполучений із першим суматором за модулем два [Патент США № US2003/0063741, МПК H04K1/04, 3.04.2003 р.].

Недоліками способу-найближчого аналога є те, що режим зчеплення блоків зашифрованого тексту є слабким до атак "дня народження" і "зустрічі по середині", за рахунок яких порушується цілісність повідомлення і не забезпечується достатній рівень криптографічної стійкості.

В основу корисної моделі поставлена задача створення пристрою для шифрування даних в режимі зчеплення блоків даних, в якому за рахунок

(19) UA (11) 61270 (13) U

використання випадкового зчеплення поточного блоку відкритого тексту із групою попередніх блоків відкритих текстів та зашифрованих текстів досягається можливість протидіяти атакам "дня народження" і "зустрічі по середині", що призводить до підвищення криптографічної стійкості процесу шифрування.

Поставлена задача вирішується тим, що в пристрій для шифрування даних в режимі зчеплення блоків даних, що містить оперативно запам'ятовуючий пристрій, сполучений із першим регістром даних, першим суматором за модулем два, що сполучений із криптографічним процесором, сполучений із другим суматором за модулем два, сполучений із оперативно запам'ятовуючим пристроєм, перший пристрій логічного множення, сполучений із першим суматором за модулем два, другий пристрій логічного множення, сполучений із другим суматором за модулем два, другий регістр даних, додатково введено комутатор, пристрій додавання за модулем 2^n, третій суматор за модулем два, третій регістр даних, генератор псевдовипадкових послідовностей бітів, при цьому перший регістр даних сполучений із комутатором, сполучений із пристроєм додавання за модулем 2^n, сполучений із третім регістром даних, першим і другим пристроями логічного множення, третій регістр даних сполучений Із пристроєм додавання за модулем 2^n, другий суматор за модулем два сполучений із другим регістром даних, сполучений із комутатором, генератор псевдовипадкових послідовностей бітів сполучений із третім суматором за модулем два, сполучений із керуючим входом комутатора.

На кресленні зображена схема пристрою, який реалізує процес шифрування даних в режимі зчеплення блоків даних.

Пристрій для шифрування даних в режимі зчеплення блоків даних містить ОЗП 1, вихід якого сполучено із першим входом першого суматора за модулем два 2, входом першого регістра даних 3, вихід якого сполучено із першим входом комутатора 4, другий вхід якого сполучено Із виходом другого регістру даних 5, вихід комутатора 4, сполучено із першим входом пристрою додавання за модулем 2^n 6, вихід якого сполучено із входом третього регістра даних 7, другим входом першого 8 і першим входом другого 9 пристроїв логічного множення, вихід третього регістра даних 7 сполучено із другим входом пристрою додавання за модулем 2^n 6, вихід першого пристрою логічного множення 8 сполучено із другим входом першого суматора за модулем два 2, вихід якого сполучено із входом КП 10, вихід якого сполучено із другим входом другого суматора за модулем два 11, вихід якого сполучено із входом ОЗП 1 та входом другого регістра даних 5, вихід другого пристрою логічного множення 9 сполучено із першим входом другого суматора за модулем два 11, вихід генератора псевдовипадкових послідовностей бітів 12. сполучено із другим входом третього суматора за модулем два 13, вихід якого сполучено із керуючим входом комутатора 4.

Пристрій для шифрування даних в режимі зчеплення блоків даних працює таким чином.

На початковому етапі роботи пристрою в перший 3, другий 5 і третій 7 регістри даних надсилають нуль, через ОЗП 1 надсилають секретний ключ шифрування в КП 10. У КП 10 на основі секретного ключа шифрування формують раундові ключі, що використовують під час виконання операцій зашифрування/розшифрування даних. Другий вхід другого пристрою логічного множення 8, на який подають керуючий сигнал є інверсним.

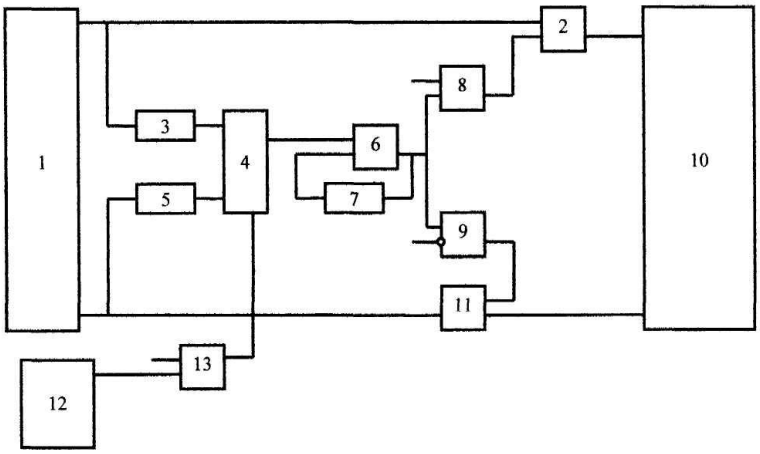
Зашифрування блока даних виконують таким чином. Через ОЗП і в перший регістр даних 3 та в КП 10 через перший суматор за модулем два 2 надсилають вектор ініціалізації, який зашифровують і через другий суматор за модулем два 11 надсилають в другий регістр даних 5.

На перший вхід третього суматора за модулем два 13, перший вхід першого 8 та другий вхід другого 9 пристроїв логічною множення надсилають сигнал керування, логічну "1", який встановлює режим зашифрування даних. Із виходу генератора псевдовипадкових послідовностей бітів 12, надсилають випадковий біт на другий вхід третього суматора за модулем два 13, який додають за модулем два із значенням керуючого сигнал, отриманий результат надходить на керуючий вхід комутатора 4. Якщо на керуючий вхід комутатора 4 надходить логічний "0", то через перший вхід комутатора 4, значення з виходу першого регістра даних 3 надсилають на вихід комутатора 4. Якщо на керуючий вхід комутатора 4 надходить логічна "1", то через другий вхід комутатора 4, значення з виходу другого регістра даних 5 надсилають на вихід комутатора 4. Значення з виходу комутатора 4 надсилають на перший вхід пристрою додавання за модулем 2^n 6 та додають із значенням, що надходить на другий вхід пристрою додавання за модулем 2^n 6 із виходу третього регістра даних 7. Отриманий результат надходить на вхід третього регістра даних 7 та другий вхід першого пристрою логічного множення 8. Через ОЗП І на вхід першого регістра даних 3 та перший вхід першого суматора за модулем два 2 надсилають блок відкритого тексту, який додають із значенням, яке надходить із виходу першого пристрою логічного множення 8 на другий вхід першого суматора за модулем два 2. Значення з виходу першого суматора за модулем два 2 надходить на вхід КП 10, де його зашифровують. Зашифрований блок даних через другий суматор за модулем два 11 надсилають на вхід ОЗП 1 та вхід другого регістра даних 5 із виходу КП 10.

Розшифрування блока даних виконують таким чином. В КП 10 через перший суматор за модулем два 2 надсилають вектор ініціалізації, який зашифровують і через другий суматор за модулем два 11 надсилають в ОЗП 1. В перший 3, другий 5 і третій 7 регістри даних надсилають нуль. Через ОЗП і в перший регістр даних 3 та в КП 10 через перший суматор за модулем два 2 надсилають зашифрований вектор ініціалізації, який розшифровують, отриманий результат через другий суматор за модулем два 11 надсилають в другий регістр даних 5.

На перший вхід третього суматора за модулем два 13, перший вхід першого 8 та другий вхід дру-

гого 9 пристроїв логічного множення надсилають сигнал керування, логічний "0", який встановлює режим розшифрування даних. Із виходу генератора псевдовипадкових послідовностей бітів 12, надсилають випадковий біт на другий вхід третього суматора за модулем два 13, який додають за модулем два із значенням керуючого сигнал, отриманий результат надходить на керуючий вхід комутатора 4. Якщо на керуючий вхід комутатора 4 надходить логічний "0", то через перший вхід комутатора 4, значення з виходу першого регістра даних 3 надсилають на вихід комутатора 4. Якщо на керуючий вхід комутатора 4 надходить логічна "1", то через другий вхід комутатора 4, значення з виходу другого регістра даних 5 надсилають на вихід комутатора 4. Значення з виходу комутатора 4 надсилають на перший вхід пристрою додавання за модулем 2^n 6 та додають із значенням, що надходить на другий вхід пристрою додавання за модулем 2^n 6 із виходу третього регістра даних 7. Отриманий результат надходить на вхід третього регістра даних 7 та перший вхід другого пристрою логічного множення 9. Через ОЗП 1 на вхід першого регістра даних 3 та через перший суматор за модулем два 2 на вхід КП 10 надсилають блок зашифрованого тексту, де його розшифровують. Розшифрований блок даних надходить на другий вхід другого суматора за модулем два 11 із виходу КП 10, де його додають із значенням, яке надходить з виходу другого пристрою логічного множення 9 на перший вхід другого суматора за модулем два 11. Відкритий блок даних надсилають на вхід ОЗП 1 та вхід другого регістра даних 5.



Комп'ютерна верстка Л. Ціхановська Підписне Тираж 24 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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