МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

УКРАЇНА **(19) UA** **(11) 128611** **(13) U**

(51) МПК
H04L 9/18 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2018 03873**
(22) Дата подання заявки: **10.04.2018**
(24) Дата, з якої є чинними права на корисну модель: **25.09.2018**
(46) Публікація відомостей про видачу патенту: **25.09.2018, Бюл.№ 18**

(72) Винахідник(и):
Баришев Юрій Володимирович (UA),
Караван Владислав Русланович (UA)
(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) СПОСІБ ПСЕВДОНЕДЕТЕРМІНОВАНОГО ПОТОЧНОГО ШИФРУВАННЯ

(57) Реферат:

Спосіб псевдонедетермінованого поточного шифрування полягає в тому, що використовують групу вторинних генераторів псевдовипадкових чисел, послідовність рівномірно розподілених випадкових чисел генерують блоками по M чисел, кожен з блоків формують генератором, що визначають за допомогою допоміжної випадкової послідовності чисел відрізка [1, k]. Елемент послідовності в блоці, що породжують j-им вторинним генератором псевдовипадкових чисел, визначають шляхом обчислення $S_j(0+t)$, віддаленого від деякого визначеного символу $S_j(0)$ на випадкову величину $t \in [0,(M-1)]$. Для кожного j-го вторинного генератора псевдовипадкових чисел формують окрему послідовність псевдовипадкових чисел t_{ij} за допомогою j-го первинного генератора псевдовипадкових чисел, вибір того з k вторинних генераторів псевдовипадкових чисел, вихід якого використовується для формування і-го елемента гами, здійснюють на основі послідовності рівномірно розподілених чисел відрізка [1, k], які можуть повторюватись у вибірці з k елементів послідовності. Елемент псевдовипадкової послідовності чисел накладають на елемент інформаційних даних за допомогою пристрою додавання за модулем два.

UA 128611 U

Корисна модель належить до обчислювальної техніки і може бути використана в системах криптографічного захисту, що використовують поточне шифрування.

Відомий спосіб двоконтурного поточного шифрування - [патент України № 10775 від 25.07.2013 р., м. кл. H04L 9/18, бюл № 14, 2013 р.], який полягає в тому, що гама в першому контурі шифрування утворюється шляхом композиції даних на виході генератора стохастичної послідовності рівномірно розподілених чисел і генератора псевдовипадкової послідовності, отримана таким чином гама накладається на відкритий текст, утворюючи шифротекст першого контуру шифрування, після цього кожне слово отриманого шифротексту розщеплюється на два півслова, які визначають стан стохастичного генератора другого контуру шифрування, символи з виходу якого видаються у відкритий канал зв'язку одержувачу інформації.

Недоліком аналога є використання лише двох генераторів для формування гами, яка потім накладається на відкритий текст.

Найбільш близьким до способу, що пропонується є спосіб формування послідовності рівномірно розподілених випадкових чисел - [патент України № 8072 від 10.01.2014 р., М. кл. G06F 7/58, бюл № 1, 2014 р.], в якому на відрізку $[0,(2^n-1)]$ випадкових чисел, що використовує групу з k різних генераторів випадкових n-розрядних чисел з періодами, рівними $M=2^n$, в подальшому вторинними генераторами псевдовипадкових чисел, причому послідовність рівномірно розподілених випадкових чисел генерується блоками по M чисел, кожен з блоків формується генератором, що визначається за допомогою допоміжної випадкової послідовності k неповторюваних чисел відрізка [1,k], елемент послідовності в блоці, що породжується і-тим генератором, визначається шляхом обчислення символу $S_i(0+t)$, віддаленого від деякого визначеного символу $S_i(O)$ на випадкову величину $t\in[0,(M-1)]$, при цьому значення t для кожного символу в блоці визначається з допоміжної послідовності M неповторюваних чисел відрізка [0,(M-1)], над числами допоміжних послідовностей k неповторюваних чисел відрізку [1,k] і M неповторюваних чисел відрізку [0,(M-1)] виконуються операції перестановки після формування кожних k блоків і M символів (одного блока), відповідно.

Недоліком прототипу є недостатня стійкість до розкриття, що обумовлено тим, що числа на відрізку [1,k] є неповторюваними, а отже кожен з вторинних генераторів псевдовипадкових чисел завжди приймає однакову участь у формуванні вихідної послідовності чисел, при цьому місце в послідовності "заплутується" лише перестановкою, чого недостатньо для задач криптографічного перетворення.

В основу корисної моделі поставлена задача створення способу псевдонедетермінованого поточного шифрування, в якому за рахунок використання псевдонедетермінованого способу формування гами приховується від криптоаналітика номер біту з гами кожного з вторинних генераторів псевдовипадкових чисел, який використовується як біт вихідної гами всього пристрою генерування гами, що використовується у способі, а також участь кожного з вторинних генераторів псевдовипадкових чисел в процесі формування вихідної послідовності, що сприяє збільшенню стійкості генератора до розкриття.

Поставлена задача вирішується за рахунок того, що в способі псевдонедетермінованого поточного шифрування використовують групу з k різних генераторів випадкових n-розрядних чисел, в подальшому вторинних генераторів псевдовипадкових чисел, послідовність рівномірно розподілених випадкових чисел генерують блоками по M чисел, кожен з блоків формують генератором, що визначається за допомогою допоміжної випадкової послідовності чисел відрізка [1,k], елемент послідовності в блоці, що породжується j-им вторинним генератором псевдовипадкових чисел, визначають шляхом обчислення $S_i(0+t)$, віддаленого від деякого визначеного символу $S_i(0)$ на випадкову величину $t\in [0,(M-1)]$, причому для кожного j-го вторинного генератора псевдовипадкових чисел формують окрему послідовність псевдовипадкових чисел t_{ij} за допомогою j-го первинного генератора псевдовипадкових чисел, вибір того з k вторинних генераторів псевдовипадкових чисел, вихід якого використовується для формування і-го елемента гами, здійснюють на основі послідовності рівномірно розподілених чисел відрізка [1,k], які можуть повторюватись у вибірці з k елементів послідовності, елемент псевдовипадкової послідовності чисел накладають на елемент інформаційних даних за допомогою пристрою додавання за модулем два.

На кресленні наведена схема пристрою, що реалізує спосіб псевдонедетермінованого поточного шифрування.

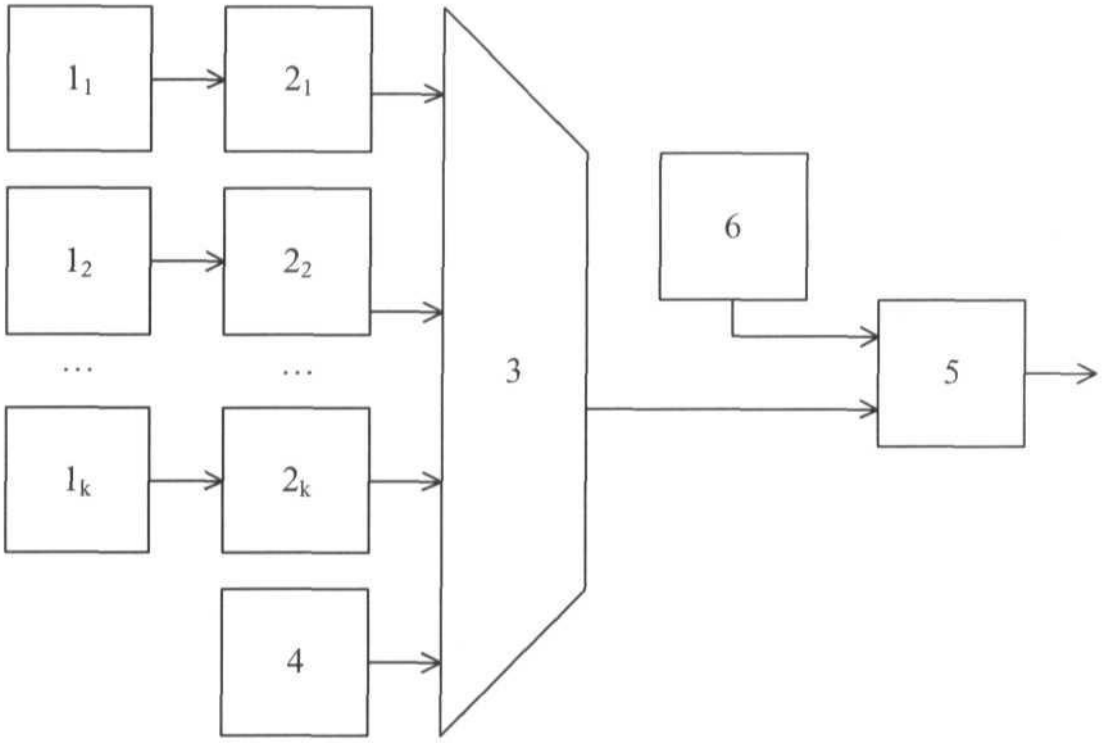
Схема містить первинні генератори псевдовипадкових чисел 1_1, 1_2,…, 1_k, виходи яких є входами для вторинних генераторів псевдовипадкових чисел 2_1, 2_2,…, 2_k. Виходи вторинних генераторів псевдовипадкових чисел 2_1, 2_2,…, 2_k є інформаційними входами мультиплексора 3. Керуючі входи мультиплексора 3 з'єднані з виходом генератора псевдовипадкових чисел 4. Входами пристрою додавання за модулем два 5 є вихід мультиплексора 3 та вхід регістру

зберігання відкритого тексту 6. Вихід пристрою додавання за модулем два 5 є виходом всього пристрою.

Спосіб псевдонедетермінованого поточного шифрування реалізується таким чином. Первинні генератори псевдовипадкових чисел 1_1, 1_2,…, 1_k, вторинні генератори псевдовипадкових чисел 2_1, 2_2,…, 2_k та генератор псевдовипадкових чисел 4 встановлюють у початкові стани, які визначають на основі ключа шифрування. Починають ітеративний процес. З виходу j-го первинного генератора псевдовипадкових чисел 1_j (j=1, 2,…, k) отримують значення кількості робочих ітерацій формування біту гами q_i для j-го вторинного генератора псевдовипадкових чисел 2_i. За допомогою j-го вторинного генератора псевдовипадкових чисел 2_i виконують q_i ітерацій формування псевдовипадкового біту. Значення біту, отриманого з виходу вторинного генератора псевдовипадкових чисел 2_i після q_i-ї генерації, надсилають на j-й інформаційний вхід мультиплексора 3. Формують псевдовипадкове ціле число в діапазоні [1,k] за допомогою генератора псевдовипадкових чисел 4 та надсилають його значення на керуючий вхід мультиплексора 3, тим самим визначаючи той з k сформованих елементів послідовності, який подається на пристрій додавання за модулем два 5. Також на вхід пристрою додавання за модулем два 5 подають елемент послідовності інформаційних даних з регістру зберігання відкритого тексту 6 в результаті чого відбувається процес накладання гами. Зсувають регістр зберігання відкритого тексту 6 на одну позицію. Починають наступну ітерацію. Після завершення обробки всіх даних з регістру зберігання відкритого тексту 6 зупиняють ітеративний процес. На кожній ітерації з виходу пристрою додавання за модулем два 5 отримують біт шифротексту.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб псевдонедетермінованого поточного шифрування, який полягає в тому, що використовують групу вторинних генераторів псевдовипадкових чисел, послідовність рівномірно розподілених випадкових чисел генерують блоками по M чисел, кожен з блоків формують генератором, що визначають за допомогою допоміжної випадкової послідовності чисел відрізка [1, k], елемент послідовності в блоці, що породжують j-им вторинним генератором псевдовипадкових чисел, визначають шляхом обчислення $S_j(0+t)$, віддаленого від деякого визначеного символу $S_j(0)$ на випадкову величину $t \in [0,(M-1)]$, який **відрізняється** тим, що для кожного j-го вторинного генератора псевдовипадкових чисел формують окрему послідовність псевдовипадкових чисел t_{ij} за допомогою j-го первинного генератора псевдовипадкових чисел, вибір того з k вторинних генераторів псевдовипадкових чисел, вихід якого використовується для формування i-го елемента гами, здійснюють на основі послідовності рівномірно розподілених чисел відрізка [1, k], які можуть повторюватись у вибірці з k елементів послідовності, елемент псевдовипадкової послідовності чисел накладають на елемент інформаційних даних за допомогою пристрою додавання за модулем два.



Комп'ютерна верстка Л. Литвиненко

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

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