



УКРАЇНА

(19) **UA** (11) **61188** (13) **U**
(51) МПК (2011.01)
H04L 9/00
H04B 7/22 (2006.01)

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СПОСІБ НЕЗАЛЕЖНОГО ФОРМУВАННЯ ВИПАДКОВОЇ ЧИСЛОВОЇ ПОСЛІДОВНОСТІ, ОДНАКОВОЇ У ДВОХ РОЗНЕСЕНИХ ПУНКТАХ

1

(21) u201015709

(22) 27.12.2010

(24) 11.07.2011

(46) 11.07.2011, Бюл.№ 13, 2011 р.

(72) АНТІПОВ ІВАН ЄВГЕНІЙОВИЧ, КОСТИРЯ
ОЛЕКСАНДР ОЛЕКСІЙОВИЧ, ТКАЛІЧ ІННА ОЛЕ-
КСАНДРІВНА

(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИ-
ТЕТ РАДІОЕЛЕКТРОНІКИ

2

(57) Спосіб незалежного формування випадкової числової послідовності, однакової у двох рознесених пунктах, який полягає у вимірюванні випадкової для даного метеорного радіовіддзеркалення характеристики, який **відрізняється** тим, що випадковій числовій послідовності приписаний випадковий часовий інтервал виникнення метеорних слідів у часі.

Корисна модель належить до радіотехніки, а саме до криптографічної техніки, і може бути використана в системах зв'язку для захисту інформації від несанкціонованого доступу.

Відомий спосіб дистанційної генерації ключа (Пат. України №40880 МПК H04L9/00, H04B7/22, опублікований 27.04.2009 Бюл. №8), в якому ключ не передається від першого абонента до другого, а створюється на сторонах метеорного радіоканалу, що передає та приймає, одночасно шляхом вимірювання одного й того ж процесу, до якого криптоаналітик (або інший абонент) не має доступу. Принцип генерації ключа полягає у тому, що у пунктах системи метеорного зв'язку, що передає та приймає, визначається фазово-кутомірним способом випадкова для даного метеорного радіовіддзеркалення характеристика - кутові координати метеорного сліду, причому для визначення координат у першому пункті використовується сигнал другого пункту, а для визначення координат у другому пункті використовується сигнал першого пункту.

Недоліком даного винаходу є те, що для його реалізації необхідно обмінюватися сигналами у двох рознесених пунктах, які можуть бути перехоплені третьою стороною.

Найбільш близьким за сукупністю ознак, що заявляються, є спосіб дистанційної генерації ключа (Пат. РФ №2265957 МПК H04B7/22, H04L9/20, опублікований 10.12.2005 Бюл. №34), що використовується для метеорного радіозв'язку, який ґрунтується на вимірюванні випадкової для даного

метеорного радіовіддзеркалення характеристики - часі розповсюдження сигналу від передавача до приймача.

Недоліком цього способу є те, що в пунктах передачі та прийому необхідно мати високоточні синхронізовані еталони часу, які мають значну вартість.

Основою корисної моделі є завдання формування випадкової числової послідовності, в якій ключ формується без додаткової передачі сигналів від першого абонента до другого і навпаки, а формується на підставі вимірювання часового інтервалу між радіовіддзеркаленнями від метеорних слідів без використання високоточних еталонів часу.

Такий технічний результат досягається тим, що у способі незалежного формування випадкової послідовності, однакової у двох рознесених пунктах, який полягає у вимірюванні випадкової для даного метеорного радіовіддзеркалення характеристики, згідно корисної моделі, випадковій числовій послідовності приписаний випадковий часовий інтервал виникнення метеорних слідів у часі.

На фігурі зображена структурна схема пристрою, яка реалізує заявлений спосіб.

Пристрій складається з передавача 1, пристрою формування імпульсів 2, кварцевого годинника 3, антени 4, приймача 5, видільника переднього фронту 6, вимірника інтервалу між попереднім і черговим метеорним слідами 7, формувача ключа 8, пристрою, що шифрує та дешифрує 9. На структурній схемі зображено два іденти-

(19) **UA** (11) **61188** (13) **U**

чні комплекти, які встановлюють у пунктах зв'язку А і В.

На виході передавача 1 знаходиться антена 4, вхід передавача 1 сполучений з другим виходом формувача імпульсів 2, до входу формувача імпульсів 2 приєднаний кварцевий годинник 3, при цьому другий вихід сполучений з першим входом вимірника інтервалу між попереднім і черговим метеорним слідами 7, приймач 5 сполучений входом з антеною 4 і виходом з входом видільника переднього фронту 6, який виходом сполучений з другим входом вимірника інтервалу між попереднім і черговим метеорним слідами 7, вихід якого сполучений з входом формувача ключа 8, вихід якого сполучений з входом пристрою, що шифрує та дешифрує 9.

Спосіб можна реалізувати наступним чином.

Передавач 1 пункту А випромінює сигнал, який згенерований формувачем імпульсів 2, що тактується кварцевим годинником 3. Після віддзеркалення від метеорного сліду сигнал приймається антенною 4 пункту В. Завдяки високій швидкості наростання амплітуди сигналу при формуванні сліду (400-500 дБ/с) видільник переднього фронту

6 однозначно визначає його початок і оповіщає про цю подію вимірника інтервалу між попереднім і черговим метеорним слідами 7. Вимірник інтервалу представляє собою лічильник, що тактується кварцевим годинником 3, який у момент початку сигналу передає значення інтервалу формувачу ключа 8 і обнуляється. На основі набутого значення відповідно до заданого методу формування ключа формувач 8 обчислює ключ для пристрою, що шифрує та дешифрує 9. Передавана інформація шифрується цим ключем у пристрої, що шифрує та дешифрує 9 і далі поступає в канал зв'язку.

У пункті В виконуються ті ж самі дії, які викладені вище, відмінність полягає у тому, що у пункті А шифрується сформованим ключем інформація, що передається у канал зв'язку, а в пункті В за допомогою сформованого ключа дешифрується отримана з каналу зв'язку інформація.

На підставі інформації про часові інтервали між окремими радіовіддзеркаленнями від метеорних слідів за допомогою пристрою формування ключа 8 можна отримати випадкові числові послідовності, які є однакові у двох рознесених пунктах А і В.

