



УКРАЇНА

(19) **UA** (11) **40880** (13) **U**
(51) МПК (2009)
H04L 9/00
H04B 7/22

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

2

(21) u200814112

(22) 08.12.2008

(24) 27.04.2009

(46) 27.04.2009, Бюл.№ 8, 2009 р.

(72) АНТІПОВ ІВАН ЄВГЕНІЙОВИЧ, UA, КОСТИРЯ
ОЛЕКСАНДР ОЛЕКСІЙОВИЧ, UA, ШЕРНІН МИ-
ХАЙЛО ОЛЕКСАНДРОВИЧ, UA

(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИ-
ТЕТ РАДІОЕЛЕКТРОНІКИ, UA

(57) Спосіб незалежного формування випадкової
числової послідовності, однакової у двох рознесе-

них пунктах, що полягає у визначенні фазово-
кутомірним способом кутових координат метеор-
ного сліду з двох просторово рознесених пунктів,
причому для визначення координат у першому
пункті використовується сигнал другого пункту, а
для визначення координат у другому пункті вико-
ристовується сигнал першого пункту, який **відріз-
няється** тим, що випадковій числовій послідовно-
сті приписане випадкове положення метеорного
сліду в просторі, яке обчислюється за знайденими
кутовими координатами.

Корисна модель відноситься до галузі радіо-
техніки, а саме до криптографічної техніки, та мо-
же бути використаний у системах зв'язку для захи-
сту інформації від несанкціонованого доступу.

Відомий спосіб дистанційної генерації ключа
[Пат. РФ №2265957 МПК H04B7/22, H04L9/20,
опубл. 10.12.2005 Бюл. №34], у якому ключ не пе-
редається від першого абонента до другого, а
створюється на сторонах передавача та приймача
метеорного радіоканалу одночасно шляхом виміру
одного і того ж процесу, до якого криптоаналітик
(або інший абонент) не має доступу. Принцип ге-
нерації ключа полягає у тому, що на приймачі та
на передавачі системи метеорного зв'язку вимірю-
ється випадкова для даного метеорного радіовід-
биття характеристика - час розповсюдження сиг-
налу від передавача до приймача.

Недоліком даної корисної моделі є те, що в
пунктах передачі та прийому необхідно мати висо-
коточні синхронізовані еталони часу, які мають
значну вартість.

Найбільш близьким за сукупністю ознак, що
заявляється, є спосіб визначення координат мете-
орного сліду [Пат. України №67664 А МПК
G04G7/02, опубл. 15.06.04. Бюл. №6, 2004р.], який
використовується для метеорного радіозв'язку
(або синхронізації шкал часу), що полягає у вико-
ристанні фазово-кутомірному способу визначення
кутових координат метеорного сліду з двох прост-
орово рознесених пунктів. Для визначення кутो-

вих координат метеорного сліду в першому пункті
радіолінії метеорного зв'язку (або синхронізації
шкал часу) використовують сигнал другого пункту,
а для визначення кутових координат у другому
пункті використовують сигнал першого пункту.

Однак недоліком цього способу є те, що він не
формує випадкових послідовностей у двох розне-
сених пунктах.

В основу корисної моделі поставлена задача
формування випадкової числової послідовності,
яка після цього може бути використана як ключ.

Такий технічний результат досягається тим,
що у способі незалежного формування випадкової
числової послідовності однакової у двох рознесе-
них пунктах, що полягає у визначенні фазово-
кутомірним способом кутових координат метеор-
ного сліду з двох просторово рознесених пунктів,
при чому для визначення координат у першому
пункті використовується сигнал другого пункту, а
для визначення координат у другому пункті вико-
ристовується сигнал першого пункту, згідно корис-
ної моделі, випадковій числовій послідовності при-
писано випадкове положення метеорного сліду в
просторі, яке обчислюється за знайденими куто-
вими координатами.

На Фіг.1 зображена структурна схема при-
строю, що реалізує заявлений спосіб. На Фіг.2, 3
зображені відповідно вертикальна та горизонталь-
на проекції схеми радіолінії метеорного зв'язку, де

(13) **U**

(11) **40880**

(19) **UA**

кути $\alpha_1, \beta_1, \alpha_2, \beta_2$, що вимірюються з пунктів зв'язку А і В, є базою для формування випадкової числової послідовності однакової у двох рознесених пунктах.

Пристрій складається з передавача 1, пристрою формування ключів 2, обчислювального пристрою 3, фазового кутоміра 4, приймача 5, фазованої антенної решітки 6. На структурній схемі зображені два ідентичних пристрої, що встановлюються у пунктах зв'язку А і В.

На виході передавача 1 знаходиться антена, вхід передавача 1 з'єднаний з другим виходом обчислювального пристрою 3, до першого входу обчислювального пристрою 3 приєднаний фазовий кутомір 4, у свою чергу вхід фазового кутоміра 4 приєднаний до фазованої антенної решітки 6, другий вихід якої з'єднаний з входом приймача 5 та вихід якого з'єднаний з другим входом обчислювального пристрою 3, який першим виходом з'єднано з пристроєм формування ключів 2, вихід якого є виходом пристрою в цілому.

Спосіб може бути реалізовано таким чином.

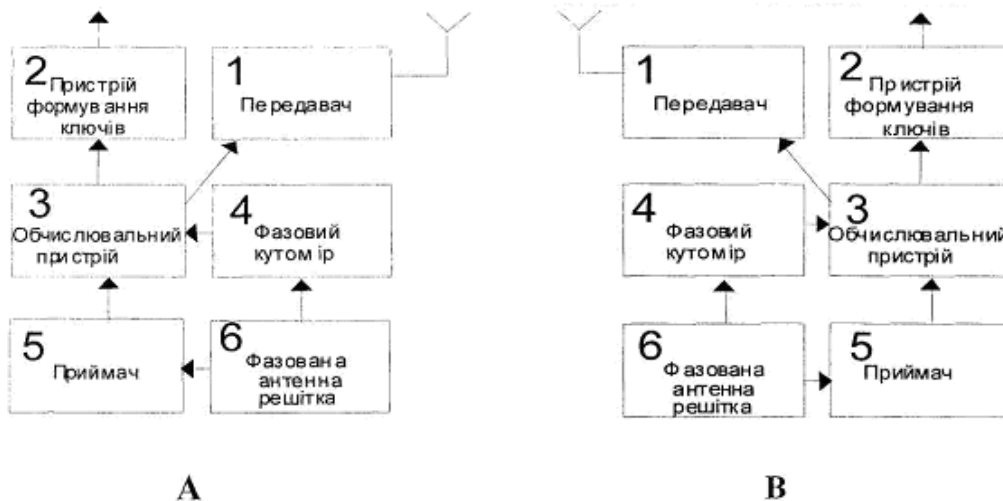
Зонduючий сигнал від передавача 1 пункту А випромінюється передавальною антеною та після відбиття від метеорного сліду М приймається фазовою антенною решіткою пункту В, після чого надходить на приймач 5 та фазовий кутомір 4 пункту В. Приймач 5 фіксує факт прийому сигналу від

пункту А та формує керуючий сигнал, що надходить на другий вхід обчислювального пристрою 3. Від фазового кутоміра 4 інформація про різницю фаз між сигналами, прийнятими різними елементами фазованої антенної решітки 6, надходить на перший вхід обчислювального пристрою 3. Обчислювальний пристрій 3 за різницею фаз визначає кути α_2, β_2 на метеорний слід. З першого виходу обчислювального пристрою 3 інформація надходить на пристрій формування ключів 2, у якому і формуються ключі. З другого виходу обчислювального пристрою 3 інформація про кути α_2, β_2 надходить до передавача 1, який через антену передає її до пункту зв'язку А.

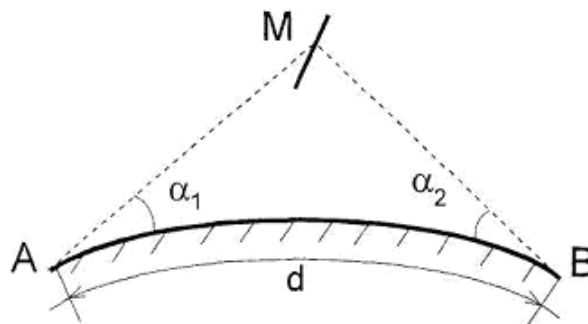
У пункті А виконуються всі дії, що наведені попередню, однак джерелом сигналу для пункту А є передавач пункту В. В результаті виконаних дій у пункті А визначаються кути α_1, β_1 .

Приймач 5 пункту А приймає інформацію про кути α_2, β_2 від пункту В, що теж надходять на обчислювальний пристрій 3.

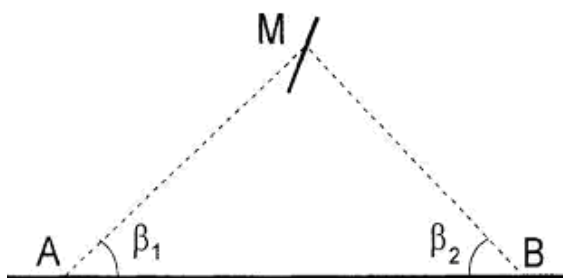
На підставі інформації про кути $\alpha_1, \beta_1, \alpha_2, \beta_2$ за допомогою пристрою формування ключів 2 створюємо незалежні випадкові числові послідовності однакової у двох рознесених пунктах А і В.



Фиг. 1



Фиг. 2



Фіг. 3