



УКРАЇНА

(19) UA (11) 71056 (13) C2
(51) 7 H04N7/167МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ НА ВІНАХІД

(54) СПОСІБ ТА СИСТЕМА ДЛЯ ПЕРЕДАВАННЯ ШИФРОВАНОЇ ІНФОРМАЦІЇ

1

(21) 2002076227
(22) 24.01.2001
(24) 15.11.2004
(86) PCT/IB01/00094, 24.01.2001
(31) 0166/00
(32) 28.01.2000
(33) CH
(31) 60/226,769
(32) 21.08.2000
(33) US
(46) 15.11.2004, Бюл. № 11, 2004 р.
(72) Кудельські Андре, СН, Сасселі Марко, СН
(73) НАГРАКАРД С.А., СН
(56) EP 0583202, 16.02.1994
EP 0461029, 11.12.1991
(57) 1. Багатоканальна система передавання шифрованої інформації для платного телебачення, яка містить центр управління і принаймні один абонентський блок, де центр управління передає зашифровані сигнали та одноканальні повідомлення (ЕСМ) щодо перевірки повноважень, зашифровані для кожного каналу, яка **відрізняється** тим, що вона містить багатоканальні повідомлення (МЕСМ) щодо перевірки повноважень, спільні для групи каналів, причому ці повідомлення поєднуються з одноканальними повідомленнями (ЕСМ) щодо перевірки повноважень для того каналу, який приймається в даний момент, з метою дешифрування сигналів та повідомлень.
2. Багатоканальна система передавання за п. 1, яка **відрізняється** тим, що багатоканальні повідомлення (МЕСМ) щодо перевірки повноважень шифруються алгоритмом, який відрізняється від алгоритму, використаного для шифрування одноканальних повідомлень (ЕСМ) щодо перевірки повноважень.
3. Багатоканальна система передавання за пунктами 1 і 2, яка **відрізняється** тим, що багатоканальні повідомлення (МЕСМ) щодо перевірки повноважень змінюються протягом періоду, що відрізняється від періоду для одноканальних повідомлень (ЕСМ) щодо перевірки повноважень.
4. Багатоканальна система передавання за пунктами від 1 до 3, яка **відрізняється** тим, що інформація, яка міститься в багатоканальних повідомленнях (МЕСМ) щодо перевірки повноважень, поєднується з інформацією, яка міститься в одноканальних повідомленнях (ЕСМ) щодо перевірки

2

повноважень, шляхом таких операцій, як додавання, віднімання або виключення (виключне АБО), множення або кодування.

5. Багатоканальна система передавання за пунктами від 1 до 3, яка **відрізняється** тим, що абонентський блок містить шифрувальний блок (СУ), який з одноканальних повідомлень (ЕСМ) щодо перевірки повноважень визначає керуючі слова (CW), дозволяючи тим самим абонентському блоку дешифрувати зашифровані сигнали, причому зміст багатоканальних повідомлень (МЕСМ) щодо перевірки повноважень поєднується з параметрами (P1, P2 ... Pn), призначеними для криптографічних розрахунків, які виконуються шифрувальним блоком (СУ).

6. Спосіб передавання багатоканальних зашифрованих сигналів для платного телебачення, який складається з:

- передавання багатоканальних зашифрованих сигналів до абонентського блока,
- передавання одноканальних повідомлень (ЕСМ) щодо перевірки повноважень, зашифрованих для кожного каналу,
- дешифрування повідомлень (ЕСМ) щодо перевірки повноважень для каналу, який приймається в даний момент, з допомогою шифрувального блока (СУ), причому дешифрована інформація надає керуючі слова (CW), необхідні для дешифрування сигналів, що відповідають каналу, який приймається в даний момент, який **відрізняється** тим, що він полягає в:

- передаванні багатоканальних повідомлень (МЕСМ) щодо перевірки повноважень, спільних для групи каналів,
- дешифруванні цих багатоканальних повідомлень (МЕСМ) щодо перевірки повноважень та у поєднанні цієї дешифрованої інформації з інформацією, необхідною для одержання керуючих слів (CW).

7. Спосіб передавання багатоканальних зашифрованих сигналів за п. 6, який **відрізняється** тим, що поєднання здійснюється із вхідними параметрами (P1, P2 ... Pn) шифрувального блока (СУ).

8. Спосіб передавання багатоканальних зашифрованих сигналів за п. 6, який **відрізняється** тим, що поєднання здійснюється з результатами, отриманими шифрувальним блоком (CD).

(13) C2

(11) 71056

(19) UA

9. Спосіб передавання багатоканальних зашифрованих сигналів за пунктами від 6 до 8, який **відрізняється** тим, що він полягає у зміні багатоканальних повідомлень (MECM) щодо перевірки повноважень протягом періоду, який відрізняється від періоду зміни одноканальних повідомлень (ECM) щодо перевірки повноважень.

10. Спосіб передавання багатоканальних зашифрованих сигналів за пунктами від 6 до 9, який **відрізняється** тим, що він полягає у шифруванні багатоканальних повідомлень (MECM) щодо перевірки повноважень з допомогою алгоритму, який відрізняється від алгоритму, використаного для шифрування одноканальних повідомлень (ECM) щодо перевірки повноважень.

Даний винахід стосується способу та системи для передавання шифрованої інформації (даних) між системою управління та декодером абонента.

Декодери абонентів платного телебачення містять блок дешифрування, який здатний обробляти сигнали, що надходять по кабелю або через бездротові засоби зв'язку. Ці сигнали можуть бути аналоговими або цифровими.

Це сигнали різних видів, і відповідно вони містять аудіо-, відео- або керуючу інформацію.

До інформації останньої категорії відносяться адміністративні повідомлення (так звані EMM повідомлення про надання права), тобто повідомлення, які містять керуючі дані, призначені для декодера або групи декодерів, та керуючі повідомлення (так звані ECM повідомлення), тобто такі, які, крім іншого, містять повідомлення щодо перевірки повноважень, а саме, інформація, яка дозволяє розшифрувати сигнали передачі.

Дана заявка стосується повідомлень (ECM) щодо перевірки повноважень, призначених для дешифрування аудіо- та відеосигналів.

Абонентам платного телебачення пропонується багато каналів, кожен з яких зашифровано з допомогою одного або більшої кількості спеціальних ключів. Це потрібно для того, щоб абонент міг користуватися підпискою на певний канал, не маючи прав на користування іншими каналами.

Повідомлення (ECM) щодо перевірки повноважень шифруються ключем, пристосованим під систему управління. Декодер абонента містить захищений шифрувальний блок, здатний розшифрувати такі повідомлення. З метою безпеки інформація щодо перевірки повноважень, яка дозволяє розшифрувати корисні сигнали (відео і аудіо), періодично змінюється. Система управління передає такі повідомлення (ECM) у зашифрованому вигляді до шифрувального блоку, що здатний дешифрувати ці повідомлення, проводить перевірку повноважень абонента і відповідно до його прав передає на декодер інформацію, необхідну для дешифрування відео- та аудіосигналів.

Результат дешифрування з допомогою шифрувального блоку називається "керуючим словом", яке позначається аббревіатурою "CW". Керуючі слова управляють декодером, і таким чином, абонент може у повній мірі скористатися переданою інформацією.

Як зазначено вище, керуючі слова регулярно змінюються, аби відвернути можливість для пірата вирахувати цю керівну інформацію з допомогою потужного комп'ютера і безоплатно скористуватися платною послугою. Саме тому керуючі слова

регулярно змінюються з періодом, зазвичай, від 1 до 20 секунд. Цей період зветься крипто-періодом.

Повідомлення (ECM) щодо перевірки повноважень посилаються з частотою, більшою за крипто-період, наприклад, кожні 100 мілісекунд. Це є необхідною умовою, з одного боку, для початку дешифрування, а з іншого боку, для зміни каналів.

Дійсно, аби мати змогу проглянути бажану передачу, необхідно в своєму розпорядженні мати керуючі слова для дешифрування сигналів. Недоречно очікувати 5 секунд перед екраном, доки з'явиться чітке зображення.

У другому випадку, коли для кожного каналу наявні керуючі слова, необхідно чекати кінця крипто-періоду для того, щоб одержати повідомлення щодо перевірки повноважень, яке дозволяє дешифрувати сигнали нового каналу. Так само, як і щойно зазначено, не можна погодитися на затримку в кілька секунд при зміні каналу.

Ось чому, на практиці, повідомлення (ECM) щодо перевірки повноважень посилаються з частотою від 5 до 20 повідомлень за секунду.

При перемиканні каналу час, що розділяє замовлення абонента і появу бажаного каналу на екрані, повинен бути щонайменшим. Згідно з існуючими стандартами прийнятного вважається тривалість порядку 500 мілісекунд.

Протягом цього проміжку часу виконуються наступні операції:

- розміщення на новому каналі аудіо-, відео- та керуючих програм-фільтрів;

- очікування наступного повідомлення (ECM), яке містить зашифроване керуюче слово для згаданого каналу;

- приймання цього повідомлення (ECM) і його передавання до блоку шифрування для дешифрування; та

- виконання алгоритму дешифрування блоком шифрування і повернення дешифрованого керуючого слова, передавання цього слова на декодер;

- початок розпаковування алгоритму стиснення рухомого зображення (MPEG) і очікування появи повністю синхронізованого зображення.

З розгляду ланцюга цих операцій видно, що вони не можуть виконуватися паралельно, а отже, у випадку перемикання каналів для кожної з них необхідно визначити максимальну тривалість.

Відомо, що чим більш високий ступінь захисту алгоритму шифрування, тим довші операції, необхідні для його дешифрування. З іншого боку, час дешифрування, який безпосередньо пов'язаний з розрахунком тривалості перемикання каналів, не може бути збільшеним з метою підвищення якості

шифрування. Саме тому ці обмеження в часі вимушено лімітують ступінь захисту алгоритмів, використаних для одержання керуючих слів.

Відомий спосіб, який описано в документі ЕР 0583202, полягає в посиланні, по активному каналу, не лише повідомлення (ЕСМ) щодо перевірки повноважень стосовно каналу, котрий являє інтерес, але також повідомлення щодо перевірки повноважень для інших каналів. Ці останні передаються з нижчою частотою, аби не перевантажувати надмірно передачу.

Недоліками цього методу є надмірне перевантаження каналу зайвими повідомленнями і необхідність запам'ятовувати всі повідомлення щодо перевірки повноважень для їх використання у разі перемикання каналів. Іншим невирішеним аспектом цього документу є підвищення якості (а отже і тривалості) операції дешифрування, яка не повинна збільшувати час перемикання каналів.

Задачею даного винаходу є запропонувати спосіб та систему передачі зашифрованої інформації, які гарантують високий ступінь захисту для надходження керуючих слів до декодера без збільшення тривалості обробки керуючого слова, яке відповідає певному каналу.

Ця мета повністю досягається шляхом використання керуючого слова, отриманого за рахунок поєднання дешифрування повідомлення (ЕСМ) щодо перевірки повноважень для кожного каналу з дешифруванням повідомлення щодо перевірки повноважень, спільного для групи каналів.

В наступному описі повідомлення для кожного каналу називаються "одноканальними повідомленнями (ЕСМ) щодо перевірки повноважень", а повідомлення, спільні для групи каналів, називаються "багатоканальними повідомленнями (MECM) щодо перевірки повноважень" (Master ESM).

Алгоритм обробки повідомлень (ЕСМ) належить до розряду швидкодіючих, а тому забезпечує обмежений захист даних. Ця умова пов'язана з малим проміжком часу, який вимагається під час переходу з одного каналу на інший.

З іншого боку, згідно з винаходом не можливо одержати керуючі слова (CW) лише за рахунок обробки одноканальних повідомлень (ЕСМ). Шифрувальний блок, який має бути здатним дешифрувати одноканальні повідомлення (ЕСМ), повинен містити інформацію, прийняту в багатоканальному повідомленні (MECM). Остання дешифрується системою, яка викликається ключем, оскільки вона не залежить від різних каналів.

Під час комутації каналів або перемикання з одного каналу на інший інформація, що міститься в одноканальному повідомленні (ЕСМ) щодо перевірки повноважень, яке стосується нового каналу, поєднується з інформацією, яка міститься в багатоканальному повідомленні (MECM) щодо перевірки повноважень і яка вже знаходиться в шифрувальному блоці, причому остання інформація є спільною для обох цих каналів. Таким чином, тривалість дешифрування повідомлення (MECM) не стає на перешкоді розрахункам тривалості комутації, як описано вище. Тому алгоритм для дешифрування повідомлень (MECM) може бути потужнішим, а отже, потребувати більше часу, проте

без негативних наслідків для тривалості комутації. Крім того, просте використання різних алгоритмів збільшує захист системи.

Інформаційне наповнення багатоканальних повідомлень (MECM) може змінюватися залежно від періоду, схожого на крипто-період для повідомлень (ЕСМ), або залежно від кратного числа цих періодів.

Якщо час між двома одноканальними повідомленнями (ЕСМ) важливий, оскільки він безпосередньо впливає на розрахунки максимального часу комутації каналів, цього не можна сказати про час між двома багатоканальними повідомленнями (MECM). Оскільки це повідомлення є спільним для групи каналів, воно може мати більшу тривалість. Дійсно, інтервал його повторення стає на перешкоді лише в момент увімкнення декодера. Якщо поглянути на цифри, то виявляється, що достатніми є від 1 до 2 повторень цих повідомлень щосекунди.

Винахід стане більш зрозумілим завдяки наступному детальному опису з посиланням на додатні ілюстрації, які наводяться, як приклад, що не вносить обмежень, і на яких:

- Фіг.1 ілюструє передавання повідомлень (ЕСМ) і (MECM) по двох каналах А і В;

- Фіг.2 - захищений шифрувальний блок.

На Фіг.1 повідомлення, які дозволяють дешифрувати відео- та аудіосигнали показані схематично, на двох лініях. Можна бачити, що для кожного каналу передавання одноканальних повідомлень (ЕСМ) відбувається з регулярними інтервалами. По каналу "А" передаються одноканальні повідомлення (ЕСМ) "А" щодо перевірки повноважень. По каналу "В" передаються одноканальні повідомлення (ЕСМ) "В" щодо перевірки повноважень. Багатоканальні повідомлення (MECM), спільні для каналів А і В, передаються по обох каналах.

В режимі роботи з використанням аналогової телепередачі по кожному з каналів успішно передаються одноканальні і багатоканальні повідомлення щодо перевірки повноважень, причому один канал пов'язаний з однією частотою. З іншого боку, в системах цифрових телепередач поняття каналу, пов'язаного з частотою, відсутнє. Багатоканальні повідомлення (MECM) можуть бути приєднані до повідомлень для цього каналу або передані глобально в інформаційному потоці без обов'язкового їх повторення на кожному каналі.

Згідно з даним прикладом періодичність багатоканальних повідомлень (MECM) наполовину менша періодичності одноканальних повідомлень (ЕСМ). Періодичність повідомлень (MECM) визначається прийнятною тривалістю дешифрування в момент першого використання повідомлення. У цьому випадку розшифрувати сигнали можна буде після прийняття принаймні одного повідомлення (ЕСМ) і одного повідомлення (MECM). Ось чому повторення повідомлення (MECM) приблизно через одну секунду є прийнятним і не завантажує смуги пропускання системи. Як тільки повідомлення (MECM) прийняте і оброблене, воно негайно стає доступним у разі необхідності перемикання на канал з новим повідомленням (ЕСМ).

Інший аспект винаходу полягає в тому, що в ньому з самого початку враховуються зменшення

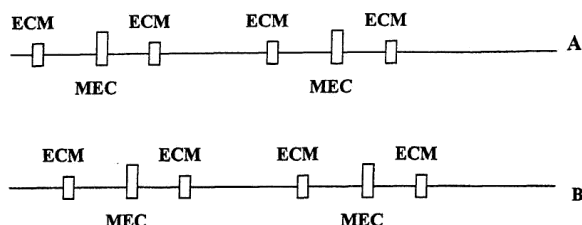
крипто-періоду залежно від каналу. Дійсно, зміна керуючого слова може бути проведена в різні моменти залежно від каналу. Тому на каналі "А", наприклад, керуюче слово (CW) змінюється з CW-A1 на CW-A2. Згідно з винаходом, у такому разі керуюче слово одержують завдяки багатоканальному повідомленню (MECM-2). З іншого боку, в припущенні, що канал В завжди працює з керуючим словом (CW-B1), необхідно буде користуватися багатоканальним повідомленням (MECM-1). Саме тому кожне повідомлення (MECM) містить інформацію про кілька крипто-періодів, що дозволяє не бути залежним від різниці у синхронізації каналів.

На Фіг.2 показані функціональні можливості цих даних, переданих у багатоканальному повідомленні (MECM). Одноканальне повідомлення (ECM), яке у зашифрованому вигляді містить керуюче слово (CW), передається до шифрувального блоку (CU), що здатний дешифрувати цю інформацію. Для цього він має у своєму розпорядженні

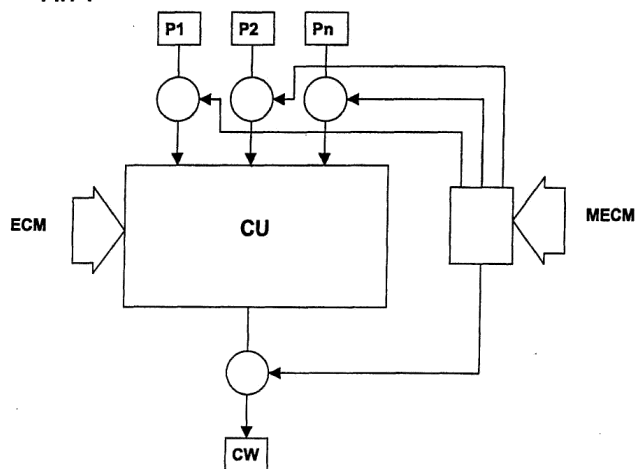
параметри P1, P2 і т.д. до Pn, які визначають права, пов'язані із системою взагалі і з даним каналом зокрема. Завдяки цим параметрам блок вираховує керуюче слово (CW). Згідно з винаходом дані, передані в повідомленні (MECM), будучи один раз дешифровані, можуть змінювати ці параметри перед шифрувальним блоком (CU) або після цього блоку.

Згідно з окремим варіантом винаходу кінцеве керуюче слово (CW) одержують з допомогою логічної операції між інформацією, що міститься в повідомленні (MECM), і повідомленням (ECM), а саме, з допомогою додавання, віднімання, виключення або множення.

Згідно з окремим варіантом винаходу інформація, що міститься в повідомленні (MECM), використовується як вторинний ключ для дешифрування інформаційного змісту одноканальних повідомлень (ECM).



Фіг. 1



Фіг. 2