

Цей винахід стосується системи мовлення й приймання, зокрема (але не виключно), систем цифрового інтерактивного супутникового телебачення для масового споживача. Він стосується також приймача-декодера і пристрою дистанційного керування для нього.

Більш конкретно, винахід, що пропонується, стосується систем так званого платного телебачення і/або радіомовлення, в яких користувач/глядач вибирає для перегляду програму/фільм/гру, яка повинна бути оплачена, що називається оплатою за перегляд (PPV - Pay Per View, оплата проводиться за кожну переглянугу передачу) або, у разі завантаження даних - оплатою за файл, або пофайловою оплатою (PPF - Pay Per File).

У таких відомих PPV- або PPF-системах кінцевому користувачеві/глядачеві спочатку необхідно взаємодіяти із системою, не тільки для того, щоб вибрати продукт, що підлягає постачанню, але також у певних випадках і для того, щоб сплатити це постачання. Термін "продукт" використовується в цьому випадку для позначення будь-якої програми, фільму або іншого об'єкта (передачі) або даних, що підлягають передаванню, або в телевізор кінцевого користувача, або в персональний комп'ютер, підключений до системи.

Цей винахід стосується також системи для здійснення дистанційних купівель і системи для надання дистанційних банківських послуг, в яких для здійснення якої-небудь транзакції, наприклад, для купівлі товару або послуги, що рекламується, застосовується, нарівні з мовною інформацією, кредитна або банківська картка.

Цей винахід пропонує пристрій, що включає в себе приймач-декодер для використання при прийманні телевізійної або радіопрограми або файла даних, і включає засіб для взаємодії із кредитною або банківською картою користувача, для зчитування інформації, що знаходиться на згаданій картці.

Така структура може спростити оплату продуктів, вимагаючи мінімальних дій з боку користувача.

Банківська або кредитна картка може містити дані на магнітній смужці (або іншому "пасивному" носії даних). Однак у варіанті, якому віддається найбільша перевага, банківська або кредитна картка має мікропроцесор (або інший "активний" пристрій зберігання інформації), і згаданий пристрій виконаний з можливістю взаємодії з цим мікропроцесором, і у варіанті, якому віддається перевага, виконаний із можливістю передавання інформації в цей мікропроцесор. Завдяки цьому може бути забезпечений більш високий рівень захищеності, і може бути спрощена передача інформації.

У варіанті, якому віддається перевага, згаданий пристрій додатково включає в себе засіб для передавання у віддалений центр команди дебетування, базуючись на згаданій інформації, що міститься на картці, для здійснення дебетування кредитного або банківського рахунку користувача.

В одній переважній реалізації згаданий пристрій виконаний з можливістю приймання від згаданого віддаленого центру інформації щодо санкціонування, а також керування декодуванням і/або дескремблюванням згаданої програми або файла в залежності від цієї інформації щодо санкціонування. Завдяки цьому може бути спрощено надання PPV- і PPF-сервісів.

В одній з реалізацій, якій віддається перевага, згаданий пристрій додатково включає в себе засіб для взаємодії зі смарт-карткою, що містить інформацію, що стосується передплати, при цьому керування декодуванням і дескремблюванням здійснюється в залежності від згаданої інформації, що стосується передплати. Смарт-картка може також містити інформацію, що стосується ключа дешифрування, а також інформацію про канали, передплачені користувачем.

У варіанті, якому віддається перевага, згаданий пристрій виконаний із можливістю збереження в пам'яті згаданої смарт-картки інформації про "кредити" для приймання, що представляє відомості про наявні "кредити", які можуть бути використані для придбання продуктів, і у варіанті, якому віддається перевага, він включає в себе засіб для зміни згаданої інформації про "кредити" для приймання, з метою зменшення наявних "кредитів" на певну величину у відповідь на приймання певної програми або файла. Таким чином, користувач може зберігати "кредити" для придбання продуктів (PPV-програм або PPF-файлів) на смарт-картці.

В одній з реалізацій, яким віддається перевага, згаданий пристрій виконаний із можливістю передавання команд дебетування, у варіанті, якому віддається перевага - за запитом користувача, в згаданий віддалений центр, і змінювання згаданої інформації, що зберігається на смарт-картці, про "кредити" для приймання, у варіанті, якому віддається перевага, після приймання інформації щодо санкціонування, з метою збільшення кількості "кредитів", збережених на смарт-картці, в залежності від платежу, здійсненого за допомогою згаданої банківської або кредитної картки. Таким чином користувач може, використовуючи банківську або кредитну картку, купувати "кредити", що зберігаються на смарт-картці для подальшого використання.

В варіанті, якому віддається найбільша перевага, згаданий пристрій виконаний із можливістю придбання "кредитів", достатніх для забезпечення можливості придбання множини продуктів, при кожній транзакції, при якій у віддалений центр передається команда дебетування; завдяки цьому може бути скорочена кількість необхідних транзакцій з участю віддаленого центра, і може бути підвищена безпека, шляхом зменшення кількості операцій, що вимагають передавання відомостей з банківської або кредитної картки.

В одній із реалізацій, особливо зручній для системи для здійснення дистанційних купівель, згаданий пристрій включає в себе засіб для обробки даних, що характеризують згадану банківську або кредитну картку користувача, разом із прийнятими даними, що характеризують товар або послугу, що пропонується, і для передавання запиту з замовленням у віддалений центр для обробки. За допомогою такої системи можуть бути спрощені замовлення й оплата продуктів, що рекламуються. У варіанті, якому віддається перевага, передбачається засіб для введення користувачем запиту на придбання продукту або послуги, що демонструється на екрані; це може спростити процес здійснення купівлі до такого ступеня, що користувачеві буде треба тільки підтвердити, що він бажає придбати який-небудь конкретний товар.

Пристрій може додатково включати в себе засіб для приймання особистого ідентифікаційного номера (PIN), у варіанті, якому віддається перевага, асоційованого зі згаданою кредитною або банківською картою, що у варіанті, якому віддається перевага, передається від пристрою віддаленого доступу з дотриманням заходів безпеки для санкціонування транзакції.

У варіанті, якому віддається перевага, згаданий пристрій виконаний у вигляді телевізійної приставки (STB

- Set-Top-Box), що являє собою, у варіанті, якому віддається перевага, автономний блок, який включає в себе як схеми декодера, так і схеми пристрою зчитування карт. У той же час згаданий пристрій може бути вбудованим у телевізор, відеоманітофон або пристрій типу комп'ютера.

Цей винахід застосовується, в варіанті, якому віддається найбільша перевага, для приймання програм або файлів, що передаються за допомогою супутника, і, зокрема - цифрових супутникових програм, оскільки в цьому випадку передбачені можливості для передавання даних, хоч, звичайно, він застосовний також для кабельних і наземних систем.

Особливістю, якій віддається особлива перевага, є те, що згаданий пристрій включає в себе додатковий засіб взаємодії для взаємодії з (додатковою) картою користувача для зчитування інформації, що знаходиться на цій картці, причому згаданий засіб є відокремленим від згаданого засобу для взаємодії із кредитною або банківською картою користувача. Завдяки застосуванню двох пристроїв зчитування карток корисні властивості пристрою можуть бути додатково підвищені.

Цей важливий аспект надається незалежно. Таким чином, згідно з ще одним спорідненим аспектом даного винаходу, пропонується пристрій, що включає в себе приймач-декодер для використання при прийманні телевізійної або радіопрограми або файла даних, засіб для взаємодії із кредитною або банківською картою користувача, для зчитування інформації, що знаходиться на згаданій картці, і, окремо від згаданого засобу, додатковий засіб взаємодії для взаємодії з картою користувача з метою зчитування інформації, що знаходиться на цій картці.

В варіанті, якому віддається перевага, згаданий додатковий засіб взаємодії виконаний із можливістю взаємодії з картою, що включає в себе мікропроцесор, і згадана картка є так званою "смарт-картою". В варіанті, якому віддається найбільша перевага, згаданий пристрій виконаний із можливістю передавання інформації у згаданий мікропроцесор.

Згідно з ще одним аспектом цього винаходу, пропонується приймач-декодер для використання в системі цифрового супутникового телебачення, який включає в себе декодер і засіб для приймання кредитної або банківської картки з мікропроцесором, а також засіб для взаємодії із згаданим мікропроцесором коли згадана кредитна або банківська картка встановлена в робоче положення в приймачі-декодері, для забезпечення зчитування даних, що знаходяться на згаданій кредитній або банківській картці, і введення даних в мікропроцесор згаданої кредитної або банківської картки.

Згідно з особливістю цього додаткового аспекту цього винаходу, якій віддається перевага, згаданий приймач-декодер включає в себе також засіб для приймання смарт-картки, причому встановленням смарт-картки кінцевим користувачем у приймач-декодер забезпечується можливість взаємодії смарт-картки із згаданим приймачем-декодером, завдяки чому певний вибраний кінцевим користувачем продукт може бути доставлений в згаданий приймач-декодер і з нього в телевізор або персональний комп'ютер, до якого може бути підключений цей приймач-декодер.

Згідно з ще одним аспектом цього винаходу пропонується система цифрового супутникового телебачення або радіомовлення, що включає в себе множину терміналів кінцевих користувачів, кожний з яких включає в себе приймач-декодер, описаний в будь-якому із двох попередніх абзаців.

Цей винахід також пропонує використання пристрою зчитування кредитних або банківських карт спільно із пристроєм для приймання або декодування радіо- або телевізійних сигналів, у варіанті, якому віддається перевага, сигналів супутникового телебачення, з метою надання інформації, що дозволяє за запитом на програму, файл, товар або послугу, що пропонується, дебетувати кредитний або банківський рахунок користувача.

У аспекті, що відноситься до способу, цим винаходом пропонується спосіб виведення програми або надання можливості завантаження файла, що включає, в приймачі-декодері, що приймає інформацію, що відноситься до згаданого файла або програми, зчитування із кредитної або банківської картки інформації, визначення того, чи має користувач права на приймання згаданої програми або файла, і якщо має, виведення згаданої програми або надання можливості завантаження згаданого файла і видачу команди дебетування для дебетування кредитного або банківського рахунку користувача. У варіанті реалізації, якому віддається перевага, фактичне дебетування кредитного або банківського рахунку звичайно виконується перед відображенням згаданої програми або наданням можливості завантаження згаданого файла.

У ще одному аспекті, що відноситься до способу, цим винаходом пропонується спосіб розміщення замовлення на який-небудь товар або послугу, що включає, в приймачі-декодері, що приймає інформацію про згаданий товар або послугу, зчитування із кредитної або банківської картки інформації, формування запиту з замовленням, який містить інформацію, яка ідентифікує згаданий товар або послугу, і інформацію, що представляє відомості кредитної або банківської картки, і передавання інформації замовлення у віддалений центр для обробки.

У варіанті, якому віддається перевага, згаданий спосіб включає також, у віддаленому центрі, обробку згаданої інформації замовлення і прийняття рішення щодо санкціонування даної транзакції виходячи із згаданої інформації з кредитної або банківської картки.

Що стосується згаданого вище пристрою, у варіанті, якому віддається перевага, він додатково включає в себе пристрій дистанційного керування, для передавання особистого ідентифікаційного номера (PIN) користувача в згаданий приймач-декодер. У варіанті, якому віддається більша перевага, згаданий пристрій дистанційного керування включає в себе засіб забезпечення безпеки для забезпечення безпеки передавання. Ці особливості будуть описані детальніше нижче.

У аспекті винаходу, що описується зараз, цей винахід відноситься також до пристрою дистанційного керування для предмета обладнання, і, більш конкретно, до ручного пристрою дистанційного керування, що використовується для керування телевізорами, приймачами-декодерами для систем супутникового телебачення і іншим подібним обладнанням.

Функціонування таких пристроїв керування засновано на передаванні сигналу від згаданого ручного пристрою керування в згаданий предмет обладнання; одним зі способів здійснення цього є використання

інфрачервоного випромінення.

Як обговорювалося раніше, для надання користувачеві можливості здійснення транзакцій, пов'язаних із купівлями і банківськими операціями, за допомогою телевізійної системи, користувачеві для здійснення фінансової транзакції необхідно вводити так званий особистий ідентифікаційний номер (PIN). Номер PIN користувача повинен, звичайно, залишатися відомим тільки даному користувачеві, щоб треті особи не мали можливості без дозволу переводити кошти з банківського рахунку користувача. При використанні відомих пристроїв дистанційного керування інформація, що передається від ручного пристрою в телевізор, може бути перехоплена; це становить проблему у разі передавання конфіденційних даних. Метою цього винаходу є розв'язання даної проблеми, із збереженням при цьому природи операцій, що виконуються користувачем, як можна більш простою.

Цей аспект цього винаходу стосується, зокрема, надання ручного пристрою дистанційного керування, який може бути використаний із телевізійною системою, за допомогою якої можуть здійснюватися фінансові транзакції.

Відповідно до цього аспекту цього винаходу пропонується пристрій дистанційного керування для певного предмета обладнання, який включає в себе засіб, за допомогою якого в цей предмет обладнання може бути переданий особистий ідентифікаційний номер (PIN) користувача, і який включає в себе засіб забезпечення безпеки для забезпечення безпеки згаданого передавання.

У вельми спорідненому аспекті цим винаходом пропонується пристрій дистанційного керування для певного предмета обладнання, що включає в себе засоби, що визначають корпус згаданого пристрою керування, засіб для передавання особистого ідентифікаційного номера (PIN) користувача в згаданий предмет обладнання, і засіб забезпечення безпеки, для забезпечення безпеки згаданого передавання.

У варіанті, якому віддається перевага, згаданий засіб передавання включає в себе засіб для формування інфрачервоного променя; завдяки цьому забезпечується зручний засіб передавання, який менш схильний до перехоплення, ніж інші передавальні середовища.

У варіанті, якому віддається перевага, згаданий засіб забезпечення безпеки включає в себе засіб для шифрування згаданого номера PIN; завдяки цьому можна перешкодити визначенню номера PIN, якщо передача буде перехоплена.

Згаданий засіб шифрування може включати в себе засіб для комбінування згаданого номера PIN із певним випадковим числом (або псевдовипадковим числом); завдяки цьому несанкціоноване дешифрування може бути утруднене.

Може бути передбачений засіб, що дозволяє користувачеві вводити згадане випадкове число; надання можливості введення користувачем може знизити здатність до перехоплення згаданого випадкового числа.

Буде зручним, якщо згаданий засіб введення включає в себе щонайменше одну клавішу для введення згаданого випадкового числа і додаткову клавішу, при цьому згаданий пристрій керування виконаний з можливістю передавання номера PIN за допомогою згаданого засобу передавання тільки після натиснення на цю додаткову клавішу. Така реалізація проста в експлуатації, і при цьому надійна, компактна і забезпечує безпеку.

Буде корисним, якщо згаданий засіб шифрування включає в себе засіб для збереження згаданого випадкового числа в згаданому пристрої керування; це спростує кодування номера PIN, що вводиться згодом.

Згаданий засіб забезпечення безпеки може включати в себе засіб для генерування числової характеристики даного конкретного пристрою керування, для її передавання за допомогою згаданого засобу передавання в згаданий предмет обладнання. Така реалізація може забезпечувати більш високий ступінь безпеки і може також перешкодити використанню несанкціонованих пристроїв дистанційного керування.

Подібним чином, для підвищення ступеня безпеки згаданий засіб шифрування може включати в себе засіб для формування числової характеристики даного конкретного пристрою дистанційного керування і засіб для комбінування згаданого числової характеристики із згаданим випадковим числом і згаданим номером PIN.

У реалізації, якій віддається перевага, згаданий засіб шифрування включає в себе засіб для приймання певного випадкового числа від згаданого предмета обладнання і засіб для комбінування згаданого випадкового числа з номером PIN користувача, для передавання за допомогою згаданого засобу передавання в згаданий предмет обладнання. Це може зробити шифрування більш надійним, завдяки тому, що випадкове число надається тільки коли воно необхідне для шифрування.

У варіанті, якому віддається перевага, згаданий пристрій керування включає в себе також засіб для передавання команд керування для згаданого обладнання і, у варіанті, якому віддається перевага, засіб введення, що функціонує селективно, в залежності від стану згаданого пристрою дистанційного керування по введенню, або для введення згаданого номера PIN, або для введення команди керування для згаданого обладнання, при цьому згаданий стан по введенню встановлюється відповідно до додаткового засобу введення. Згаданий засіб введення може включати в себе числову клавішу введення, і команда керування може містити команду вибору каналу або програми. Згаданий додатковий засіб введення може включати в себе додаткову функціональну клавішу.

Цим винаходом також пропонується набір, який включає пристрій дистанційного керування, описаний вище, і згаданий предмет обладнання, причому згаданий предмет обладнання включає в себе засіб для приймання номера PIN користувача.

У такому наборі згаданий предмет обладнання може включати в себе засіб для генерування випадкового числа і засіб для виведення згаданого випадкового на пристрій відображення; завдяки цьому спростується введення випадкового числа під час шифрування.

Згаданий предмет обладнання може включати в себе засіб для генерування випадкового числа і засіб для передавання згаданого випадкового числа в згаданий пристрій дистанційного керування; завдяки цьому усувається необхідність введення згаданого випадкового числа вручну.

У ще одному аспекті цього винаходу пропонується система цифрового телебачення, що включає в себе предмет телевізійного обладнання, що має засіб для приймання номера PIN користувача, і пристрій

дистанційного керування, описаний вище.

У ще одному величезному спорідненому аспекті пропонується система цифрового телебачення, що включає в себе предмет телевізійного обладнання, який включає в себе засіб для приймання номера PIN, і пристрій дистанційного керування, що включає в себе засоби, які визначають корпус згаданого пристрою керування, засіб для передавання номера PIN користувача в згаданий предмет обладнання, і засіб забезпечення безпеки для забезпечення безпеки згаданого передавання.

Згаданим предметом телевізійного обладнання може бути телевізор або приймач-декодер, що підключається до телевізора.

Винахід розповсюджується також на спосіб введення номера PIN в телевізійну систему, який включає застосування пристрою дистанційного керування, описаного вище.

Нижче особливості даного винаходу, яким віддається перевага, будуть описані, виключно у вигляді прикладу, з використанням прикладених фігур, на яких:

На фіг.1 представлена загальна архітектура системи цифрового телебачення згідно з варіантом здійснення цього винаходу, якому віддається перевага;

На фіг.2 представлена архітектура системи умовного доступу згаданої системи цифрового телебачення;

На фіг.3 представлена структура повідомлення керування правами (EMM), що використовується в згаданій системі умовного доступу;

На фіг.4 представлено схематичне зображення апаратних засобів системи санкціонування передплатників (SAS) згідно з одним із варіантів здійснення цього винаходу, яким віддається перевага;

На фіг.5 представлено схематичне зображення архітектури SAS;

На фіг.6 приведена архітектура системи забезпечення інтерактивності, приведеної на фіг. 1 системи цифрового телебачення;

Фіг.7 - це схематичне зображення пристрою дистанційного керування, що використовується в системі цифрового телебачення;

На фіг.8 представлено схематичне зображення приймача-декодера згідно з винаходом, що пропонується, в перспективі;

На фіг.9 - це зображення, у вигляді схеми, протоколів, що використовуються при здійсненні кінцевим користувачем платежів за допомогою кредитної/банківської картки;

Фіг.10 - це зображення, аналогічне показаному на фіг.7, але на ньому пунктиром показані основні внутрішні компоненти згаданого пристрою керування;

Фіг.11 - це схематичне зображення основних внутрішніх компонентів приймача-декодера;

На фіг.12 показано зображення у вигляді блок-схеми першої реалізації шифрування згідно з даним винаходом;

Фіг.13 - це блок-схема, аналогічна фіг.12, але другої реалізації шифрування;

Фіг.14 - це блок-схема, аналогічна фіг.12, але третьої реалізації шифрування;

Фіг.15 - це блок-схема, аналогічна фіг.12, але п'ятої реалізації шифрування.

Структура системи 1000 цифрового телевізійного мовлення і приймання, відповідної цьому винаходу, приведена на фіг.1. Винахід включає в себе практично звичайну систему 2000 цифрового телебачення, яка застосовує відому систему MPEG-2-компресії для передавання ущільнених цифрових сигналів. Більш детально, MPEG-2-компресор 2002 в центрі мовлення приймає потік цифрових сигналів (звичайно потік відеосигналів). Компресор 2002 підключений до мультиплексора і скремблера 2004 за допомогою каналу 2006. Мультиплексор 2004 приймає множину вхідних сигналів, компонує один або кілька потоків-носіїв і передає ущільнені цифрові сигнали в передавач 2008 центра мовлення через канал 2010, тип якого, природно, може бути різним, включаючи телекомунікаційний канали. Передавач 2008 передає електромагнітні сигнали через канал "Земля-спутник" 2012 на супутниковий транспондер 2014, де виконується їх обробка електронними засобами і мовлення через віртуальний канал "супутник-Земля" 2016 на наземний приймач 2018, що звичайно має форму тарілки, що належить кінцевому користувачеві або орендується ним. Сигнали, що приймаються приймачем 2018, передаються в суміщений приймач-декодер 2020, що належить кінцевому користувачеві або орендується ним, і підключений до телевізора 2022 кінцевого користувача. Приймач-декодер 2020 декодує ущільнений MPEG-2 сигнал в телевізійний сигнал для телевізора 2022.

Система 3000 умовного доступу сполучена з мультиплексором 2004 і приймачем-декодером 2020 і розташовується частково в центрі мовлення і частково в декодері. Вона дозволяє кінцевому користувачеві здійснювати доступ до мовних передач цифрового телебачення від одного або кількох провайдерів мовлення. У приймач-декодер 2020 може встановлюватися смарт-картка, яка може декодувати повідомлення, що відносяться до комерційних пропозицій (одна або кілька телепередач, що продаються провайдером мовлення). Використовуючи декодер і смарт-картку, користувач може купувати передачі як в режимі передплати, так і в режимі оплати за перегляд (PPV).

Система 4000 забезпечення інтерактивності, також сполучена з мультиплексором 2004 і приймачем-декодером 2020 і також розташована частково в центрі мовлення і частково в декодері, забезпечує кінцевому користувачеві можливість взаємодії з різними прикладними програмами через зворотний модемний канал 4002.

Система умовного доступу

Нижче буде описана більш детально система 3000 умовного доступу.

Як показано на фіг.2, в цілому система 3000 умовного доступу включає в себе систему санкціонування передплатників (SAS) 3002. SAS 3002 підключена до однієї або кількох систем керування передплатниками (SMS) 3004, по одній SMS для кожного провайдера мовлення, за допомогою відповідного TCP/IP-каналу 3006 (хоч в альтернативних реалізаціях замість нього можуть використовуватися канали інших типів). У альтернативному варіанті, одна або декілька SMS можуть використовуватися спільно двома провайдерами мовлення, або один провайдер може використати дві SMS тощо.

Перші пристрої шифрування у вигляді шифрувальних блоків 3008, що використовують "материнські"

смарт-картки 3008, підключені до SAS через канал 3012. Другі пристрої шифрування, також у вигляді шифрувальних блоків 3014, що використовують материнські смарт-картки 3016, підключені до мультиплексора 2004 через канал 3018. Приймач-декодер 2020 приймає "дочірню" смарт-картку 3020. Він підключений безпосередньо до SAS 3002 за допомогою комунікаційних серверів 3022 через зворотний модемний канал 4002. SAS, нарівні з іншими сигналами, за запитом передає в дочірню картку передплатні права.

Смарт-картки містять "секрети" одного або кількох комерційних операторів. "Материнська" смарт-картка шифрує різні види повідомлень, а "дочірні" смарт-картки розшифровують ці повідомлення, якщо у них є на це права.

Перший і другий шифрувальні блоки 3008 і 3014 включають в себе шасі, електронну плату VME (VME - спеціалізована операційна система ICL), програмне забезпечення якої записане в програмовному ПЗП з електричним стиранням, до 20 електронних плат і одну смарт-картку 3010 і 3016 відповідно для кожної електронної плати, одну (картка 3016) для шифрування ЕСМ і одну (картка 3010) для шифрування ЕММ.

Нижче буде описана більш детально робота системи 3000 умовного доступу системи цифрового телебачення, відносно різних компонентів телевізійної системи 2000 і системи 3000 умовного доступу.

Мультиплексор і скремблер

На фіг.1 і 2 показано, що в центрі мовлення цифровий відеосигнал спочатку ущільнюється (або швидкість передавання меншає) з використанням MPEG-2-компресора 2002. Цей ущільнений сигнал потім передається в мультиплексор і скремблер 2004 через канал 2006, для того щоб мультиплексувати його з іншими даними, такими як інші ущільнені дані.

Скремблер генерує слово керування, що використовується в процесі скремблювання і що включається в потік даних MPEG-2 в мультиплексорі 2004. Слово керування генерується всередині системи і дозволяє суміщеному приймачу-декодеру 2020 кінцевого користувача дескремблювати програму.

У потік даних MPEG-2 додаються також критерії доступу, які вказують, яким чином програма пропонується споживачам. Програма може пропонуватися як в одному з багатьох режимів "передплати", так і/або в одному з багатьох режимів "з оплатою за перегляд" (PPV). У режимі передплати кінцевий користувач передплатує одну або кілька комерційних пропозицій, або "букетів" (груп), дістаючи, таким чином, права на перегляд будь-якого каналу з цих груп. У переважному варіанті реалізації із групи каналів можна вибрати до 960 комерційних пропозицій. У режимі оплати "за перегляд" кінцевому користувачеві надається можливість купувати передачі за бажанням. Це може забезпечуватися шляхом попереднього замовлення передач ("режим попереднього замовлення") або шляхом придбання програми відразу після початку мовлення ("імпульсний режим"). У реалізації, якій віддається перевага, всі користувачі є передплатниками незалежно від режиму перегляду - передплата або PPV, але, звичайно, PPV-глядачі не обов'язково повинні бути передплатниками.

Як слово керування, так і критерії доступу використовуються для формування повідомлення керування правами (ЕСМ); це повідомлення є повідомленням, що передається застосовно до однієї скремблюваної програми; повідомлення містить слово керування (яке дозволяє дескремблювати програму) і критерії доступу для даної мовної програми. Критерії доступу і слово керування передаються на другий шифрувальний блок 3014 через канал 3018. У цьому блоці ЕСМ генерується, зашифровується і передається в мультиплексор і скремблер 2004.

Кожний сервіс, що передається провайдером мовлення в потоку даних, містить кілька різних компонент; наприклад, телепередача включає в себе відеокomпоненту, аудіокomпоненту, компоненту субтитрів тощо. Кожна з цих компонент сервісу для подальшого мовлення на транспондер 2014 скремблюється і зашифровується окремо. Для кожної скремблюваної компоненти сервісу потрібно окреме ЕСМ.

Трансляція програми

Мультиплексор 2004 приймає електричні сигнали, що містять зашифровані ЕММ, від SAS 3002, зашифровані ЕСМ — від другого шифрувального блоку 3014, і ущільнені програми - від компресора 2002. Мультиплексор 2004 скремблює програми і передає скремблювані програми, скремблювані ЕММ і скремблювані ЕСМ у вигляді електричних сигналів на передавач 2008 центра мовлення через канал 2010. Передавач 2008 передає електромагнітні сигнали на супутниковий транспондер 2014 через канал "Земля-супутник" 2012.

Приймання програм

Супутниковий транспондер 2014 приймає і обробляє електромагнітні сигнали, що передаються передавачем 2008, і передає ці сигнали на наземний приймач 2018, що звичайно має форму тарілки, що належить кінцевому користувачеві або орендується ним, через канал "супутник-Земля". Сигнали, що приймаються приймачем 2018, передаються в суміщений приймач-декодер 2020, що належить кінцевому користувачеві або орендується ним і підключений до телевізора кінцевого користувача 2022. Приймач-декодер 2020 демультимплексує сигнали для отримання скремблюваних програм із зашифрованими ЕММ і зашифрованими ЕСМ.

Якщо програма не скремблювана, тобто з потоком даних MPEG-2 повідомлення ЕСМ не передаються, приймач-декодер 2020 виконує декомпресію даних і перетворює сигнал у відеосигнал для передавання його в телевізор 2022.

Якщо програма скремблювана, приймач-декодер 2020 добуває з потоку даних MPEG-2 відповідне ЕСМ і передає це ЕСМ в "дочірню" смарт-картку 3020 кінцевого користувача. Вона вставляється в гніздо приймача-декодера 2020. Дочірня смарт-картка 3020 перевіряє, чи має користувач права на дешифрування даного ЕСМ і на доступ до даної програми. Якщо ні, то в приймач-декодер 2020 передається негативна відповідь, яка вказує, що програма не може бути дескремблювана. Якщо кінцевий користувач має такі права, ЕСМ розшифровується і добувається слово керування. Декодер 2020 може потім дескремблювати програму з використанням даного слова керування. Потім виконується декомпресія потоку даних MPEG-2 і його перетворення у відеосигнал для подальшого передавання в телевізор 2022.

Система керування передплатниками (SMS)

Система керування передплатниками (SMS) 3004 містить базу даних 3024, яка керує, крім іншого, всіма

файлами кінцевих користувачів, комерційними пропозиціями (такими як тарифи і заохочення), передплатами, відомостями, що відносяться до PPV, і даними, що стосуються споживання і санкціонування кінцевого користувача. SMS може бути фізично віддалена від SAS.

Кожна SMS 3004 передає в SAS 3002 через відповідний канал 3006 повідомлення, які спричиняють перетворення або створення повідомлень керування наданням прав (EMM), що підлягають передаванню кінцевому користувачеві.

SMS 3004 також передає в SAS 3002 повідомлення, які не передбачають якого б то не було перетворення або створення повідомлень EMM, але передбачає тільки зміну статусу кінцевого користувача (відносно санкціонування, що надається кінцевому користувачеві при замовленні продукту, або суми, на яку кінцевий користувач буде дебетований).

Як буде описано нижче, SAS 3002 передає повідомлення (що звичайно запитують інформацію, таку як інформація зворотного виклику або білінгова інформація) в SMS 3004, так що очевидно, що зв'язок між цими двома системами є двостороннім.

Повідомлення керування наданням прав (EMM)

EMM (також зване повідомленням умовного доступу) — це повідомлення, призначене для індивідуального кінцевого користувача (передплатника, або абонента) або групи кінцевих користувачів. Кожна група може містити яку-небудь задану кількість кінцевих користувачів. Така організація у вигляді групи має на меті оптимізувати використання смуги пропускання; іншими словами, звертаючись до однієї групи, можна звернутися до великої кількості кінцевих користувачів.

При застосуванні цього винаходу на практиці можуть бути використані EMM різних спеціальних типів. Індивідуальні EMM призначені для індивідуальних абонентів і звичайно використовуються при наданні PPV-сервісів; вони містять ідентифікатор групи і позицію абонента в цій групі. Так звані EMM групової передплати призначені для груп з, скажемо, 256 окремих користувачів, і використовуються звичайно для адміністрування певних передплатних послуг. Таке EMM містить ідентифікатор групи і бітовий масив абонентів групи. Аудиторні EMM призначені для всієї аудиторії глядачів і можуть, наприклад, використовуватися операторами для надання певних безкоштовних послуг. "Аудиторія глядачів" — це вся сукупність абонентів, що мають смарт-картки з однаковими Ідентифікаторами Оператора (OPI). І, нарешті, "унікальні" EMM адресовані смарт-карткам з відповідним унікальним ідентифікатором.

Структура типового EMM буде описана нижче з посиланнями на фіг. 3. Загалом, EMM, яке являє собою послідовності бітів цифрових даних, складається із заголовка 3060, власне EMM 3062 і підпису 3064. Заголовок 3060, в свою чергу, складається з ідентифікатора типу 3066 для ідентифікації типу EMM - індивідуальний, груповий, аудиторний або який-небудь інший, ідентифікатора розміру 3068, який вказує розмір EMM, необов'язкової адреси 3070 для EMM, ідентифікатора оператора 3072 і ідентифікатора ключа 3074. Власне EMM, природно, істотно розрізняється в залежності від його типу. І, нарешті, підпис 3064, який звичайно має розмір 8 байтів, містить інформацію для боротьби зі спотвореннями інших даних в EMM.

Система санкціонування передплатників (SAS)

Повідомлення, що генеруються SMS 3004, передаються через канал 3006 в систему санкціонування передплатників (SAS) 3002, яка, в свою чергу, генерує повідомлення, що підтверджують приймання повідомлень, що генеруються SMS 3004, і передає ці підтвердження в SMS 3004.

Як показано на фіг.4, на рівні апаратних засобів SAS відомим чином включає в себе мейнфрейм-комп'ютер 3050 (в варіанті реалізації, якому віддається перевага, - комп'ютер DEC), пов'язаний з однією або кількома клавіатурами 3052 для введення даних і команд, одним або кількома відеомоніторами (VDU - Visual Display Unit) 3054 для відображення вихідної інформації і засобами зберігання даних 3056. Може бути передбачена певна надмірність апаратних засобів.

На рівні програмного забезпечення в варіанті реалізації, якому віддається перевага, SAS під керуванням стандартної відкритої операційної системи VMS виконує комплекс програмних засобів, архітектура яких буде описана нижче в загальному вигляді з посиланнями на фіг.5; очевидно, що програмні засоби в альтернативному варіанті можуть бути реалізовані апаратно.

У загальному вигляді, SAS містить область гілки передплати 3100 для надання прав в режимі передплати і для щомісячного автоматичного відновлення прав, область гілки PPV (оплати за перегляд) 3200 для надання прав для PPV-передач, і інжектор EMM 3300, для передавання повідомлень EMM, що створюються в областях гілок передплати і PPV, в мультиплексор і скремблер 2004 з подальшою їх подачею в потік даних MPEG. Якщо повинні бути надані інші права, такі як права пофайлової оплати (PPF - Pay Per File) у разі завантаження комп'ютерного програмного забезпечення в персональний комп'ютер користувача, передбачаються також інші подібні області.

Однією з функцій SAS 3002 є керування правами доступу до телепередач, доступних як комерційні пропозиції в режимі передплати або таких, що продаються в режимі PPV-передач відповідно до різних комерційних режимів (режим попереднього замовлення, імпульсний режим). SAS 3002, відповідно до прав і інформації, що приймаються від SMS 3004, генерує для передплатника повідомлення EMM.

Область гілки передплати 3100 включає інтерфейс команд (CI -Command Interface) 3102, сервер технічного керування передплатниками (STM - Subscriber Technical Management) 3104, генератор повідомлення (MG -Message Generator) 3106 і шифрувальний блок (CU - Ciphering Unit) 3008.

Область гілки PPV 3200 містить сервер санкціонування (AS -Authorization Server) 3202, реляційну базу даних 3204 для зберігання необхідної інформації про кінцевих користувачів, базу даних локального чорного списку 3205, сервери баз даних 3206 для вказаної бази даних, централізований сервер 3207 замовлень (OCS - Order Centralized Server), сервер 3208 для мовних компаній (SPB), генератор 3210 повідомлення (MG), функції якого в основному ті ж, що і генератора повідомлень області гілки передплати, і тому далі детально не описуються, і шифрувальний блок 3008.

Інжектор EMM 3300 складається з множини джерел повідомлень (ME — Message Emitters) 3302, 3304, 3306 і 3308 і програмних мультиплексорів (SMUX — Software MUltipleXer) 3310 і 3312. У варіанті

реалізації, якому віддається перевага, є два ME, 3302 і 3304, для генератора повідомлень (MG) 3106, і два інших ME, 3306 і 3308, для генератора повідомлень (MG) 3210. ME 3302 і 3306 підключаються до SMUX 3310, а ME 3304 і 3308 підключаються до SMUX 3312.

Система забезпечення інтерактивності

Система 4000 забезпечення інтерактивності, що також підключена до мультиплексора 2004 і приймача-декодера 2020 і також розташована частково в центрі мовлення і частково в декодері, надає кінцевому користувачеві можливість взаємодії з різними прикладними програмами через модемний зворотний канал 4002.

На фіг.6 приведена загальна структура телевізійної системи 4000 забезпечення інтерактивності системи 1000 цифрового телебачення відповідно до цього винаходу.

Система 4000 забезпечення інтерактивності включає в себе, взагалі кажучи, чотири основних елементи:

засіб розробки 4004 в центрі мовлення або в іншому місці, що дозволяє провайдеру мовлення створювати, розробляти, налагоджувати і тестувати прикладні програми;

сервер 4006 прикладних програм і даних в центрі мовлення, сполучений з засобом розробки 4004, для надання провайдеру мовлення можливості готувати, засвідчувати автентичність і формувати прикладні програми і дані для відправлення в мультиплексор і скремблер 2004, для їх введення в потік-носії MPEG-2 (звичайно в його приватну секцію), що підлягає мовленню для кінцевого користувача;

віртуальну машину, що включає в себе підсистему реального часу (RTE - Real Time Engine) 4008, яка являє собою виконуваний код, інстальований в приймачі-декодері 2020, що належить кінцевому користувачеві або орендується ним, для забезпечення кінцевому користувачеві можливості приймати, засвідчувати автентичність, декомпресувати і завантажувати прикладні програми в робочу пам'ять декодера 2020 для виконання. Підсистема 4008 також виконує резидентні прикладні програми загального призначення. Підсистема 4008 не залежить від апаратного забезпечення і операційної системи; і

зворотний мод'ємний канал 4002, що з'єднує приймач-декодер 2020 і сервер 4006 прикладних програм і даних, для подачі сигналів, що інструктують сервер 4006 вводити дані і прикладні програми в потік-носії MPEG-2 за запитом кінцевого користувача.

Телевізійна система забезпечення інтерактивності працює з використанням "прикладних програм", які керують функціонуванням приймача-декодера і різними пристроями, що входять до його складу. Прикладні програми представлені в підсистемі 4008 як "файли ресурсів". "Модуль" - це набір файлів ресурсів і даних. Одна прикладна програма може бути складений декількома модулями. "Том пам'яті" приймача-декодера - цей простір для зберігання модулів. "Інтерфейс" використовується для завантаження модулів. Модулі можуть завантажуватися в приймач-декодер 2020 з потоку-носії MPEG-2.

Застосовно до даного опису, прикладна програма - це фрагмент комп'ютерного коду для керування високорівневими функціями (операціями) приймача-декодера 2020. Наприклад, коли кінцевий користувач позиціонує фокус пристрою дистанційного керування 2026 (детально показаного на фіг.7) на об'єкті кнопки, видимому на екрані телевізора 2022, і натискає клавішу підтвердження, виконується макрос, що відповідає цій кнопці.

Інтерактивна прикладна програма забезпечує меню і виконує команди за відповідним запитом кінцевого користувача, а також надає дані відповідно до призначення даної прикладної програми. Прикладні програми можуть бути або резидентними прикладними програмами, тобто такими, що зберігаються в ПЗП (або в FLASH-пам'яті, або іншій енергонезалежній пам'яті) приймача-декодера 2020, або які передаються шляхом мовлення і завантажуються в ОЗП або FLASH-пам'ять декодера 2020.

Прикладами прикладних програм є:

Прикладна програма ініціалізації. Приймач-декодер 2020 оснащений резидентною прикладною програмою ініціалізації, яка є набором модулів (більш детально цей термін пояснюється нижче), що адаптується і дозволяє приймачу-декодеру 2020 бути безпосередньо готовим до роботи в середовищі MPEG-2. Ця прикладна програма надає базові функції, які можуть бути при необхідності модифіковані провайдером мовлення. Вона надає також інтерфейс між резидентними прикладними програмами і прикладними програмами, що завантажуються.

Прикладна програма запуску. Прикладна програма запуску дозволяє виконуватися в приймачі-декодері 2020 будь-якій прикладній програмі, або такій що завантажуються, або резидентній. Ця прикладна програма працює як програма початкового завантаження, що виконується при надходженні послуги для того, щоб запустити прикладну програму. Прикладна програма запуску завантажуються в оперативну пам'ять і, отже, може бути легко оновлена. Вона може бути сконфігурована таким чином, що інтерактивні прикладні програми, доступні по різних каналах, можуть бути вибрані і виконані або відразу ж після завантаження, або після попереднього завантаження. У разі попереднього завантаження прикладна програма завантажуються в пам'ять 2024 і активується прикладною програмою запуску з потреби.

Програма передач. Програма передач — це інтерактивна прикладна програма, яка надає повну інформацію про програми. Наприклад, вона може містити інформацію, скажемо, про програму телевізійних передач на тиждень, що надаються кожним каналом із групи ("букета") каналів цифрового телебачення. Натисненням на клавішу пристрою 2026 дистанційного керування кінцевий користувач отримує доступ до додаткового екрана, який із перекриттям накладається на передачу, яка відображається в даний момент на екрані телевізора 2022. Цей додатковий екран являє собою браузер, що надає інформацію про поточні і наступні передачі кожного каналу групи каналів цифрового ТБ. За допомогою натиснення на іншу клавішу пристрою 2026 дистанційного керування кінцевий користувач отримує доступ до прикладної програми, яка видає на екран інформацію про програму передач на тиждень. Кінцевий користувач може також проводити пошук і сортування програм як за простими, так і за сконструйованими ним самим критеріями. Кінцевий користувач може також звертатися до безпосередньо вибраного каналу.

Прикладна програма PPV. Прикладна програма PPV - це інтерактивний сервіс, наявний на кожному PPV-каналі групи каналів цифрового ТБ із системою 3000 умовного доступу. Кінцевий користувач може звертатися

до цієї прикладної програми з використанням ТБ-гіда або браузера каналів. Крім того, ця прикладна програма запускається автоматично, як тільки на PPV-каналі виявляється PPV-передача. Потім кінцевий користувач може купити поточну програму або за допомогою своєї дочірньої смарт-картки 3020, або за допомогою сервера зв'язку 3022 (з використанням модему, телефону і кодів тонового набору, системи MINITEL або іншим подібним чином). Ця прикладна програма може бути резидентною в ПЗП приймача-декодера 2020 або завантажуватися в оперативну пам'ять приймача-декодера 2020.

Прикладна програма завантаження в ПК. Кінцевий користувач може за запитом завантажувати комп'ютерне програмне забезпечення з використанням прикладної програми завантаження в ПК.

Прикладна програма перегляду журналу. Прикладна програма перегляду журналу забезпечує періодичне мовлення відеозображень із забезпеченням користувачеві можливості навігації за допомогою кнопок на екрані.

Прикладна програма телевікторини. Прикладна програма телевікторини у варіанті, якому віддається перевага, синхронізується із програмою телевікторини, що мовиться. Наприклад, на екран телевізора 2022 видаються кілька можливих відповідей, і користувач може вибрати відповідь за допомогою пристрою 2026 дистанційного керування. Прикладна програма телевікторини може інформувати користувача, правильна його відповідь чи ні, і може підраховувати набрані користувачем очки.

Прикладна програма дистанційних купівель. У одному із прикладів прикладної програми дистанційних купівель пропозиції товарів до продажу транслюються на приймач-декодер 2020 і потім виводяться на екран телевізора 2022. За допомогою пристрою дистанційного керування користувач може вибрати для купівлі який-небудь конкретний товар. Замовлення на цей товар передається через зворотний модемний канал 4002 в сервер 4006 прикладних програм і даних або в окрему систему продажу, номер телефону якої був завантажений в приймач-декодер, можливо - з дорученням дебетувати рахунок кредитної картки, яка встановлена в одному із пристроїв 4036 зчитування карт приймача-декодера 2020.

Прикладна програма дистанційних банківських послуг. У одному із прикладів прикладної програми дистанційних банківських послуг користувач встановлює банківську картку в один із пристроїв 4036 зчитування карт приймача-декодера 2020. Приймач-декодер 2020 дзвонить банку користувача з використанням номера телефону, записаного в банківській картці користувача або такого, що зберігається в приймачі-декодері, і потім прикладна програма надає набір засобів, які можуть бути вибрані за допомогою пристрою дистанційного керування 2026, наприклад, для завантаження по телефонній лінії звіту про стан рахунку, переказу коштів з одного рахунку на інший, запитування чекової книжки тощо.

Прикладна програма Інтернет-браузера. У одному прикладі прикладної програми Інтернет-браузера інструкції від користувача, такі як запит на перегляд веб-сторінки, що має конкретний URL, вводяться з використанням пристрою дистанційного керування 2026, і вони пересилаються по зворотному модемному каналу 4002 в сервер 4006 прикладних програм і даних. Відповідна веб-сторінка потім включається в дані, що транслюються з центра мовлення і приймаються приймачем-декодером 2020 через канал "Земля-супутник" 2012, транспондер 2014 і канал "супутник-Земля" 2016, і потім виводиться на екран телевізора 2022.

Прикладні програми зберігаються в елементах пам'яті приймача-декодера 2020 і представляються у вигляді файлів ресурсів. Під файлами ресурсів розуміють файли бібліотек описів графічних об'єктів, файли бібліотек блоків змінних, файли послідовностей команд, файли прикладних програм і файли даних.

Файли бібліотек описів графічних об'єктів описують екрани, людино-машинний інтерфейс прикладної програми. Файли бібліотек блоків змінних описують структури даних, якими оперує прикладна програма. Файли послідовностей команд описують функціональні дії, що виконуються прикладною програмою. Файли прикладних програм надають точки входу для прикладних програм.

Прикладні програми, що утворюються таким способом можуть використати файли даних, такі як файли бібліотек піктограм, файли зображень, файли шрифтів, файли таблиць кольорів і файли текстів ASCII. Інтерактивна прикладна програма може також отримувати оперативні (онлайн) дані, задіюючи входи і/або виходи.

Підсистема 4008 завантажує в свою пам'ять тільки ті файли ресурсів, які необхідні їй в даний час. Ці файли ресурсів прочитуються з файлів бібліотек описів графічних об'єктів, файлів послідовностей команд і файлів прикладних програм; файли бібліотек блоків змінних записуються в пам'ять після виклику процедури завантаження модулів і залишаються там доти, поки не буде зроблений спеціальний виклик процедури вивантаження модулів.

Використання кредитної картки в телевізійній приставці

Звернемося до фіг.8; кожному кінцевому користувачеві системи, описаної з посиланням на попередні фігури, надається телевізійна приставка 2019, що включає в себе приймач-декодер 2020, за допомогою якого кінцевий користувач може взаємодіяти з системою супутникового цифрового телебачення, і за допомогою якого вибрані кінцевим користувачем продукти можуть бути передані в телевізор 2022 користувача або персональний комп'ютер користувача для завантаження в нього.

У телевізійній приставці розташовуються, крім інших елементів, декодер 2020 і модем 2021, причому декодер 2020 включає в себе пам'ять 4022.

На передній стороні приставки 2019 є слоти 2023 і 2025, в які можуть встановлюватися смарт-картка 3020 і/або кредитна/банківська картка 3017, відповідно. Слоти 2023 і 2025 мають зв'язані з ними пристрої 3019 і 3021 зчитування карток, відповідно.

Спосіб, за допомогою якого "дочірня" смарт-картка, асоційована з конкретним користувачем, взаємодіє з системою, вже описаний із посиланнями на фіг.2.

У варіанті здійснення цього винаходу, що розглядається, кінцевий користувач має можливість оплачувати вибрані продукти за допомогою кредитної/банківської картки, що у варіанті, якому віддається перевага, включає в себе мікропроцесор 3017a (так званої "смарт-картки"), звичайно в PPV- і PPF-режимах роботи системи.

Використання кредитної/банківської картки стає можливим завдяки тому, що в телевізійній приставці 2019

передбачають слот 2025, а в приймачі-декодері - відповідний засіб, що забезпечує можливість взаємодії мікропроцесора 3017а з системою загалом.

У цьому варіанті здійснення приймач-декодер включає в себе традиційний пристрій зчитування карт, який знаходиться під повним керуванням того ж процесора, що здійснює керування декодуванням і керує взаємодією зі смарт-карткою. Завдяки цьому команди дебетування легко можуть бути зв'язані з "підзарядкою" смарт-картки додатковими "кредитами" (одинацями кредиту).

Згадана взаємодія включає опитування кредитної/банківської картки з метою встановлення її автентичності, дати закінчення дії картки і факту того, чи не перевищений кредитний ліміт, встановлений для її власника, і потім дебетування рахунку, з яким асоційована дана картка (за допомогою її мікропроцесора, якщо це смарт-картка, і відповідної банківської мережі), на суму, що затрачується на придбання вибраного продукту. У разі "неінтелектуальної" магнітної картки використовується аналогічна процедура.

На фіг.9 схематично представлений протокол, який використовується для забезпечення взаємодії кредитної/банківської картки 3017 із системою, метою якого є забезпечення фінансової безпеки. Цей протокол заснований на протоколі, що застосовується в цей час в системі MINITEL, що використовується у Франції.

Цей протокол працює відносно трьох різних областей: області терміналу передплатника, або кінцевого користувача, що загалом означається як область А, області постачальника системи, що загалом означається як область В, і області банку, що загалом означається як область С. На фіг. 9 області А, В і С призначені для позначення функціональних частин системи, але не фізичних особливостей.

Як вказувалося раніше з посиланням на фіг.8, користувач має кредитну картку 3017, яка включає в себе мікропроцесор 3017а у вигляді інтегральної мікросхеми. Вона може містити також так званий секретний ключ 3015, що забезпечує безпеку подібно тому, як вже описано для смарт-картки 3020 користувача, для використання при перевірці автентичності картки.

У тому, що стосується його взаємодії із кредитною карткою 3017, приймач-декодер 2020 кінцевого користувача на функціональному рівні обладнаний засобом для обробки даних, що представляють транзакцію як таку (показано як 3029), і засобом для обробки даних, що стосуються перевірки автентичності і цілісності (показано як 3031). Область А містить також відкритий ключ.

Область В, що відноситься до компетенції постачальника системи, включає в себе SMS 3004 і комунікаційний сервер 3022, описані з посиланнями на фіг.1 і фіг.2. Сервер 3022 включає в себе також криптографічний сервер 3023, обладнаний секретним ключем.

Область С включає в себе приватну банківську мережу 3032, типові учасники якої показані позиціями 3033, 3034 і 3035. Мережа 3032 включає в себе блок 3036 керування дистанційними платежами (менеджер дистанційних платежів, telepayment manager), що містить "материнський" ключ 3037.

Нижче з посиланнями на фіг. 9 буде описана послідовність подій, які задіюються при здійсненні фінансової транзакції з використанням кредитної картки 3017. На фіг. 9 стрілки вказують різні операції, що виконуються при здійсненні платежу і видачі/інжектуванні відповідного ЕММ, що підлягає прийманню приймачем-декодером 2020 кінцевого користувача.

Установлення кредитної картки 3017 типу "смарт-картки" в приймач-декодер 2020 спричиняє виконання описаних нижче операцій; потрібно зазначити, що всі операції як правило виконуються в реальному часі, якщо не зазначено іншого:

а) Приймачем-декодером 2020 із кредитної картки 3017 добувається початкова інформація. Ця інформація включає в себе номер картки, зведення про закінчення терміну дії картки, мові країни, грошові одиниці тощо. Ця інформація завантажується в оперативну пам'ять приймача-декодера.

б) Після завантаження здійснюється перевірка згаданої інформації. Якщо інформація правильна, процес продовжується; в іншому випадку, виконання транзакції уривається.

с) Вводиться номер PIN користувача, з використанням пристрою дистанційного керування 2026, як буде описано нижче.

д) Картка перевіряє згаданий номер PIN. Якщо номер правильний, процес продовжується. Якщо він неправильний, картка робить, скажемо, ще дві або три додаткові спроби. Якщо номер неправильний і при цих додаткових спробах, виконання транзакції уривається.

е) Якщо номер PIN правильний, картка робить доступними певні додаткові області пам'яті, і інформація з цих областей завантажується в оперативну пам'ять приймача-декодера. Такою інформацією можуть бути відомості про транзакції, раніше виконані за допомогою даної картки, і їхні грошові значення.

ф) Виконується перевірка, чи не перевищили згадані транзакції відповідний кредитний ліміт користувача.

г) Якщо результат додатний (тобто відповідний ліміт не перевищується), картці передається певна інформація, що стосується поточної транзакції, така як вартість, дата, банківські реквізити тощо.

h) На основі цієї інформації картка обчислює перший числовий сертифікат, який підтверджує транзакцію. Числовий сертифікат генерується мікропроцесором картки з використанням протоколу, який використовує для генерування сертифіката, що звичайно має розмір від 30 до 40 байтів, вартість транзакції, дату, номер картки, дату закінчення дії картки, посилання на продукт і іншу інформацію такого роду.

i) Відомості про транзакцію записуються в банківську/кредитну картку.

j) Картка відключається; це є важливим, оскільки небажано, щоб картка залишалася відкритою на будь-якому з наступних кроків.

к) Встановлюється з'єднання з комунікаційними серверами 3022 системи SAS 3002 за допомогою зворотного модемного каналу 4002.

1) Для перевірки системи SAS приймачем-декодером останній генерує випадкове число (або ALEA) і передає його в комунікаційні сервери 3022.

т) Згадане випадкове число зашифровується криптографічним сервером 3023 за допомогою певного алгоритму шифрування і передається назад в приймач-декодер.

п) Приймач-декодер дешифрує згадане випадкове число, щоб пересвідчитися в його правильності.

о) За умови, що SAS перевірена, SAS (і зокрема, централізований сервер 3207 замовлень (дивись фіг.5))

із використанням SMS 3004 перевіряє, чи не занесений даний передплатник в чорний список.

p) Факультативно по базі даних, розміщених, скажемо, в центрі мовлення, виконується перевірка наявності продукту, що запитується.

q) За умови, що ніяких проблем не виявлено, згадані відомості про транзакції і перший сертифікат передаються комунікаційними серверами 3022 в блок 3036 керування дистанційними платежами приватної банківської мережі 3032.

r) Перевіряється стан кредиту кінцевого користувача, і за умови, що він задовільний, блок 3036 керування дистанційними платежами видає числовий сертифікат комунікаційним серверам 3022, обчислений таким само чином, що і перший сертифікат. Цей другий сертифікат є дозволом на купівлю блоку керування дистанційними платежами. Потрібно зазначити, що другий сертифікат необхідний не завжди, наприклад, якщо вартість транзакції менше певного порогового значення, то за таких обставин в обміні інформацією із блоком керування дистанційними платежами немає необхідності.

s) Приймання оператором другого сертифіката (звичайно у вигляді електричного сигналу) є для оператора гарантією оплати банком, і, отже, потім SAS передає відповідне EMM в приймач-декодер 2020 для санкціонування купівлі (якщо купівля являє собою купівлю передачі/програми або т.п.).

t) Приймання EMM приймачем-декодером 2020 дозволяє кінцевому користувачеві переглянути вибраний PPV-продукт на своєму телевізорі 2022 або завантажити вибраний PPF-продукт в свій персональний комп'ютер.

u) Вже не в реальному часі, SAS передає в SMS 3004 сигнал, що сповіщає про транзакцію.

v) Вже не в реальному часі, SMS передає у відповідний банк 3033, 3034 або 3035 інформацію про транзакцію, щоб повідомити, що платіж був акцептований. Банк виконує необхідні дії.

Вище було детально викладено, як можуть бути реалізовані PPV- і PPF-режими з використанням кредитної або банківської картки. У доповнення до цього, той саме пристрій зчитування кредитних або банківських карт може бути використаний при санкціонуванні інших транзакцій, наприклад, купівель товарів або послуг із використанням Прикладної програми дистанційних купівель, або забезпеченні кінцевому користувачеві можливості переглянути і змінити реквізити його банківського рахунку за допомогою Прикладної програми дистанційних банківських послуг. Пристрій дистанційного керування

Як показано на фіг.7 і фіг.10, інфрачервоний пристрій керування 2026 обладнаний корпусом 2030, на верхній стороні якого розташовані клавіші, основні з яких - клавіші керування 2031, клавіша Mute (придушення) 2032 і числові клавіші 2034, пронумеровані від "0" до "9".

Корпус включає в себе засіб 2035 для формування і передавання інфрачервоного променя (в варіанті здійснення, якому віддається перевага, інфрачервоний пристрій працює згідно зі стандартом Philips RC5), пам'ять 2036, що включає в себе як ППЗП з електричним стиранням (і/або флеш-пам'ять), так і оперативну пам'ять, і засіб 2037 керування, що включає в себе засіб 2038 шифрування. Пам'ять 2036, розмір якої відносно невеликий, використовується для зберігання (в ППЗП з електричним стиранням) різних паролів і інших ідентифікаторів (як буде описано) і (в оперативній пам'яті) змінних, що використовуються при здійсненні різних обчислень. Засіб керування є взагалі традиційним, і містить, на апаратному рівні, однокристальний мікропроцесор, такий як той, що постачається компанією Philips для пристроїв дистанційного керування і, на рівні програмного забезпечення, програмне забезпечення, резидентне в пам'яті 2036 і здатне здійснювати дії, як буде описано нижче (такі як операції складання і визначення залишку від цілочисельного ділення).

Взагалі кажучи, ручний пристрій дистанційного керування, що описується, по-перше, виконаний із можливістю передавання номера PIN користувача в телевізійну систему, звичайно через декодер, і, по-друге, пристрій дистанційного керування також обладнаний засобом для шифрування згаданого номера, що підлягає передаванню, зокрема, шляхом обчислення послідовності випадкових чисел. Враховуючи факт використання із приймачем-декодером кредитної або банківської картки, шифрування є особливо важливим.

Що стосується забезпечення безпеки (захистності) при передаванні номера PIN, потрібно зазначити, що для цього можуть бути використані декілька різних способів. Зокрема, можуть бути застосовані різні протоколи і можуть використовуватися різні способи фактичного забезпечення шифрування.

Звернемося до опису системи, приведеного з посиланнями на фіг.2 і, зокрема, до опису тієї частини системи, яка включає в себе так звані материнську і дочірню смарт-картки. Звернемося також до приведеного на фіг.11 схематичного зображення внутрішніх компонентів приймача-декодера.

Конкретні особливості ручного інфрачервоного пристрою дистанційного керування, істотні в контексті, що розглядається, пов'язані з доступом приймача-декодера 2020 до дочірньої смарт-картки 3020 і/або кредитної/банківської картки 3017. Приймач-декодер 2020 керується засобом керування 2100, який розташовується в декодері і реалізовується у вигляді поєднання апаратних засобів на базі мікропроцесора і програмного забезпечення. Цей засіб керування включає в себе засіб 2102 генерування випадкового числа і засіб 2104 для виведення цього випадкового на екран телевізора, звичайно телевізора 2022. Декодер включає в себе також, в одному варіанті здійснення, якому віддається перевага, засіб приймання інфрачервоного випромінювання 2106 (в реалізації, якій віддається перевага, - інфрачервоний пристрій, що працює у відповідності зі стандартом Philips RC5), для здійснення зв'язку з інфрачервоним пристроєм керування. Однак, в іншому варіанті здійснення, декодер включає в себе як засіб приймання, так і засіб передавання інфрачервоного випромінювання, якщо бажане передавання інформації в пристрій керування. Як згадувалося раніше, приймач-декодер включає в себе також пам'ять 2024, яка, як і у разі пристрою дистанційного керування, включає в себе як ППЗП з електричним стиранням/флеш-пам'ять, так і оперативну пам'ять. Використання цієї пам'яті аналогічно описаному тут для пристрою дистанційного керування.

На фіг.12-15 ілюструються декілька протоколів шифрування, які можуть бути використані.

Як показано на фіг.12, згідно з першим протоколом шифрування, декодер 2020 під керуванням засобу керування 2100, розташованого в самому декодері, передає електромагнітний сигнал на екран телевізора, який, в свою чергу, відображає послідовність із чотирьох цифр a_1 , a_2 , a_3 , щ від 0000 до 9999; цей крок показаний в блоці 500 на фіг.12.

Це чотиризначне число може бути або абсолютно випадковим чотиризначним числом, яке змінюється при кожному звертанні кінцевого користувача до системи, або воно може бути певним заздалегідь визначеним числом із заздалегідь згенерованих випадкових чисел. Виводиться відповідне повідомлення, що пропонує користувачеві ввести згадане випадкове число в пристрій керування 2026.

Відображення цього числа і відповідного повідомлення показане на кроці 501.

Потім, на кроці 502, користувач переглядає випадкове число a_1, a_2, a_3, a_4 на екрані телевізора 2022, і на кроці 503 вводить це число в пристрій 2026 дистанційного керування, натискаючи одночасно клавішу Mute 2032.

У варіанті здійснення, якому віддається перевага, введення здійснюється за допомогою поля цифрових клавіш 2034. У альтернативному варіанті введення може здійснюватися за допомогою будь-яких відповідних засобів введення, наприклад, активуванням голосом.

Знову ж, діючи відповідно до повідомлення на екрані телевізора, користувач за допомогою поля цифрових клавіш 2034 вводить в пристрій керування 2026 свій номер PIN. Номер PIN - це також чотиризначне число c_1, c_2, c_3, c_4 , яке являє собою номер PIN, що використовується також із дочірньою смарт-карткою 3020 і/або банківською або кредитною карткою 3017. Кроки 503 і 504 виконуються користувачем при натисненій клавіші Mute 2032.

Наступний крок включає комбінування пристроєм керування 2026 двох чотиризначних номерів a_1, a_2, a_3, a_4 і c_1, c_2, c_3, c_4 з метою отримання зашифрованого чотиризначного номера t_1, t_2, t_3, t_4 .

Нижче буде описаний спосіб обчислення цифр t_1, t_2, t_3 і t_4 .

Кожна з цифр обчислюється одним і тим же способом, так що буде розглянуте тільки обчислення t_1 .

t_1 обчислюється на основі цифр a_1 і c_1 у відповідності з таким виразом:

$$t_1 = (a_1 + c_1) \bmod 10,$$

де "mod 10" означає, що береться залишок від розподілу суми $(a_1 + c_1)$ на 10; іншими словами, береться молодша значуща цифра результату.

Як показано вище, ті ж дії проводяться для отримання чисел t_2, t_3 і t_4 . Цифри c_1, c_2, c_3 і c_4 таким чином зашифровуються, захищаючи від перехоплення при передаванні пристроєм дистанційного керування номера PIN користувача в декодер 2020.

Щойно описаний крок позначений на фіг.12 позицією 505.

Потім зашифрований номер t_1, t_2, t_3, t_4 передається із пристрою дистанційного керування в декодер, що позначено на фіг.12 позицією 506.

Після приймання чотиризначного зашифрованого номера декодер відновлює первісний чотиризначний номер c_1, c_2, c_3, c_4 . Це виконується шляхом обчислення кожної з цифр c_1, c_2, c_3, c_4 виходячи з t_1, t_2, t_3 і t_4 ; цей крок позначений на фіг.12 як блок 507. Обчислення відносно цифри c_1 проводиться за формулою

$$c_1 = (t_1 a_1 + 10) \bmod 10$$

Для обчислення інших цифр використовуються аналогічні формули.

У разі дочірньої смарт-картки 3020, наступний крок для приймача-декодера складається в порівнянні відновленого номера PIN із номером, що вже зберігається в декодері і що представляє цю дочірню смарт-картку 3020. Фактично кожна з цифр c_1, c_2, c_3, c_4 порівнюється по черзі з відповідною цифрою, що зберігається в декодері. Цей крок показаний на фіг.12 як блок 508.

Останні кроки, позначені на фіг.12 як блоки 509 і 510, означають надання доступу до системи, якщо чотиризначні номери співпадають (крок 509), і заборону доступу, якщо вони не співпадають (крок 510).

У разі кредитної або банківської картки 3017, що має власний мікропроцесор (так звана "смарт-картка"), виконується інша процедура. На кроці 508 відновлений номер PIN передається в смарт-картку для перевірки, чи дійсний цей номер PIN. Якщо це так (крок 509), виходить дозвіл на відповідну транзакцію і видається відповідний (перший) сертифікат, як описано вище. Якщо ні (крок 510), санкціонування відхиляється.

Нижче буде більш детально описане виконання кроків із 503 по 506, із використанням таблиці, в якій $a_1, a_2, a_3, a_4, c_1, c_2, c_3$ і c_4 є десятиричними цифрами від "0" до "9". Якщо користувач під час приведених в таблиці наступних кроків відпускає клавішу Mute 2032, побудова послідовності припиняється. Після цього необхідно повторити всю операцію. Потрібно зазначити, що при відпусканні користувачем клавіші Mute передається код Mute.

Вибрана клавіша	Код, що передається пристроєм керування
Mute	Mute
Mute+(a_0)	Не передається
Mute+(a_2)	Не передається
Mute+(a_3)	Не передається
Mute+(a_3)	Не передається
Mute+(c_1)	$t_1 = \bmod 10$ від $(a_1 + c_1)$
Mute+(c_2)	$t_2 = \bmod 10$ від $(a_2 + c_2)$
Mute+(c_3)	$t_3 = \bmod 10$ від $(a_3 + c_3)$
Mute+(c_4)	$t_4 = \bmod 10$ від $(a_4 + c_4)$
Не вибрана (відпускається клавіша Mute)	Mute

На фіг.13 проілюстрований другий протокол шифрування, який в основному співпадає із протоколом, вже описаним за допомогою фіг.12. Однак в протокол на фіг.13 доданий додатковий крок забезпечення безпеки.

Він позначений як блок 511 і вводиться в дію збережене в пам'яті як пристрою дистанційного керування, так і засобу керування 2100 приймача-декодера 2020 додаткове випадкове число. На практиці це число звичайно

запам'ятовується при першому використанні пристрою керування.

Це додаткове випадкове число d_1, d_2, d_3, d_4 комбінується з першим випадковим числом a_1, a_2, a_3, a_4 і номером PIN c_1, c_2, c_3, c_4 з метою отримання зашифрованого номера t_1, t_2, t_3, t_4 .

Таким чином, цей додатковий крок 511 забезпечує підвищену безпеку в порівнянні із протоколом, приведеним на фіг.12.

На фіг.14 проілюстрований третій протокол шифрування, який в основному співпадає із протоколом, вже описаним за допомогою фіг.12, але має додатковий крок 512.

У цьому протоколі пам'ять 2036 пристрою дистанційного керування містить заздалегідь записане чотиризначне число e_1, e_2, e_3, e_4 , яке є ідентифікаційною ознакою даного конкретного пристрою 2026 дистанційного керування.

Цей додатковий ідентифікаційний номер комбінується на кроці 505 із випадковим числом a_1, a_2, a_3, a_4 і номером PIN користувача c_1, c_2, c_3, c_4 з метою отримання зашифрованого номера t_1, t_2, t_3, t_4 .

Засіб керування 2100 приймача-декодера 2020 включає в себе засіб, за допомогою якого ідентифікаційний номер даного пристрою дистанційного керування e_1, e_2, e_3, e_4 може порівнюватися з номером приймача-декодера системи; якщо вони не співпадають, це означає, що пристрій керування не є таким для даного конкретного приймача-декодера, що, в свою чергу, означає, що доступ до дочірньої смарт-картки 3020 і/або банківської або кредитної картки 3017 (можливий будь-який із варіантів) приймачу-декодеру 2020 не може бути наданий.

Хоч фіг.14 ілюструє додавання кроку 512 до кроків, приведених на фіг.12, додатковий крок може бути доданий також і до протоколу, приведенного на фіг.13, так що може бути забезпечений ще більш високий ступінь безпеки. Таким чином, протоколи шифрування, приведені на фіг.12, фіг.13 і фіг.14, забезпечують послідовно зростаючий ступінь безпеки.

Нижче описується четвертий протокол шифрування, який поєднує особливості, пов'язані з додатковим випадковим числом, і особливості, пов'язані з додатковим ідентифікаційним номером, як описано вище. Однією з особливих переваг такого поєднання є те, що воно дозволяє використати більш ніж один пристрій дистанційного керування (кожний з відмінним додатковим випадковим номером) з одним приймачем-декодером, за умови, що кожний такий пристрій керування має відмінний додатковий ідентифікаційний номер.

Нижче описується спосіб, за допомогою якого об'єднуються ці дві особливості, з посиланням на послідовність дій над клавішами пристрою дистанційного керування, наведену в нижченаведеній таблиці.

Вибрана клавіша	Код, що передається пристроєм керування
Mute	Mute
Mute+(a_1)	Не передається
Mute+(a_2)	Не передається
Mute+(a_3)	Не передається
Mute+(a_4)	Не передається
Mute+(c_1)	$t_1 = \text{mod } 10$ від $(a_1 + c_1 + d_1)$
Mute+(c_2)	$t_2 = \text{mod } 10$ від $(a_2 + c_2 + d_2)$
Mute+(c_3)	$t_3 = \text{mod } 10$ від $(a_3 + c_3 + d_3)$
Mute+(c_4)	$t_4 = \text{mod } 10$ від $(a_4 + c_4 + d_4)$
Mute	Один раз Mute
Mute	Один раз e_1
Mute	Один раз e_2
Mute	Один раз e_3
Mute	Один раз e_4
Не вибрана (відпускається клавіша Mute)	Один раз Mute

Потрібно відмітити, насамперед, що забезпечується сумісність із першим протоколом шифрування (описаним із посиланням на фіг.12), так що пристрій дистанційного керування може, якщо необхідно, обмінюватися інформацією із приймачем-декодером, який може працювати тільки відповідно до першого протоколу шифрування (шляхом завдання чисел d_1 - d_4 рівними нулю). Сумісність забезпечується шляхом автоматичної передавання коду Mute відразу ж після передавання t_1 - t_4 . Таким чином, декодер, що працює згідно з першим протоколом шифрування, буде приймати всі ті коди, які необхідні для його успішного функціонування.

Після передавання команди Mute у другий раз пристрій керування передає додатковий ідентифікаційний номер e_1 - e_4 , перед тим, як передати зрештою завершальний код Mute при відпущенні клавіші Mute користувачем.

У четвертому протоколі шифрування додаткове випадкове число d_1 - d_4 комбінується з першим випадковим числом a_1 - a_4 і номером PIN c_1 - c_4 таким чином (наприклад, для t_1):

$$t_1 = (a_1 + c_1 + d_1) \bmod 10$$

Номер PIN відновлюється приймачем-декодером за такою формулою (наприклад, для c_1):

$$c_1 = (t_1(a_1 + d_1) + 10) \bmod 10$$

Згідно з тією ж наведеною вище таблицею нижче описується те, як проводиться початкове генерування і збереження згаданих додаткового випадкового числа і додаткового ідентифікаційного номера.

Випадкове число генерується приймачем-декодером точно так само, як і перше випадкове число (a_1 - a_4). Однак додаткове випадкове число (d_1 - d_4) генерується тільки один раз; потім воно зберігається в пам'яті 2036

пристрою дистанційного керування для використання у всіх випадках, коли передбачається, що здійснюється введення номера PIN із використанням пристрою дистанційного керування.

Додатковий ідентифікаційний номер (e_1 - e_4) генерується приймачем-декодером як додаткове випадкове число, і, знову ж, зберігається в пам'яті 2036 для майбутнього використання.

Коли пристрій дистанційного керування використовується в перший раз (і кожний перший раз після того, як пам'ять 2036 стирається при заміні батарейки), d_1 - d_4 і e_1 - e_4 встановлюються рівними нулю. Засіб керування 2100 приймача-декодера порівнює значення e_1 - e_4 з нулем і отримує додатний результат порівняння. Тоді засіб керування генерує повідомлення, що видається на екран телевізора, яке пропонує користувачеві ввести значення, завжди при натисненій клавіші Mute, згідно з нижченаведеною таблицею.

Вибрана клавіша	Код, що передається пристроєм керування
Mute	Mute
Mute+Pilote	Pilote
Mute+(d_1)	d_1
Mute+(d_2)	d_2
Mute+(d_3)	d_3
Mute+(d_4)	d_4
Mute+(e_1)	e_1
Mute+(e_2)	e_2
Mute+(e_3)	e_3
Mute+(e_4)	e_4
Mute+Prog	Prog
Не вибрана (відпускається клавіша Mute)	Один раз Mute

Клавіші "Pilote" і "Prog" 2031 були вибрані тому, що вони в даній процедурі ніяк не використовуються. Однак можуть бути вибрані і інші придатні клавіші.

Із наведеної таблиці видно, що у користувача запитується введення значень d_1 - d_4 і e_1 - e_4 , які видаються засобом керування і відображаються на екрані телевізора. При другому натисненні на клавішу Prog ці два набори значень (тобто додатковий пароль і додатковий ідентифікаційний номер) записуються в пам'ять 2036 пристрою дистанційного керування.

При використанні пристрою дистанційного керування у другий і подальший рази, ці записані ненульові значення додаткового пароля і додаткового ідентифікаційного номера видаються із пристрою дистанційного керування. Засіб керування приймача-декодера порівнює додатковий ідентифікаційний номер із нулем і отримує від'ємний результат. При від'ємному результаті засіб керування переходить до обчислення s_1 - s_4 за заданими значеннями a_1 - a_4 , t_1 - t_4 і d_1 - d_4 . У випадку, коли значення s_1 - s_4 вірні, засіб керування підтверджує автентичність номера PIN, і подальша обробка проводиться як описано вище. У іншому випадку відмовляється в підтвердженні автентичності.

Очевидно, що четвертий протокол шифрування надає ряд переваг. По-перше, він забезпечує більший ступінь безпеки за рахунок використання додаткового пароля (який змінюється лише відносно рідко) і за рахунок використання додаткового ідентифікаційного номера. По-друге, він дозволяє використовувати декілька пристроїв дистанційного керування для одного приймача-декодера; процедура збереження додаткового пароля і додаткового ідентифікаційного номера в пристрій дистанційного керування може бути застосована до більш ніж одному пристрою дистанційного керування. По-третє, забезпечується можливість обміну інформацією пристрою дистанційного керування із приймачами-декодерами, які можуть працювати тільки згідно з першим протоколом, за рахунок використання однакових кодів.

Як вказувалося вище, однією з цілей є спробувати як можна більше полегшити життя користувача за рахунок зменшення кількості дій, які користувач повинен зробити для здійснення фінансової транзакції за допомогою пристроїв 2026 дистанційного керування. На фіг.15 наведений ще один (п'ятий) протокол шифрування, який спрощує дії, які повинен зробити користувач. У цьому протоколі приймач-декодер 2020 спочатку генерує на кроці 500 випадкове число a_1 , a_2 , a_3 , a_4 . Однак, на відміну від протоколів на фіг.12-14, декодер 2020 потім передає випадкове число a_1 , a_2 , a_3 , a_4 в пристрій 2026 дистанційного керування за допомогою інфрачервоного випромінювання, де воно зберігається в пам'яті 2036 пристрою керування. Це проводиться замість видачі випадкового числа a_1 , a_2 , a_3 , a_4 на екран телевізора.

Інші кроки цього протоколу співпадають із кроками від 504 до 510, представленими на фіг.14.

При такій реалізації користувач повинен вводити тільки одне чотиризначне число, а саме: номер PIN користувача s_1 , s_2 , s_3 , s_4 , замість двох чотиризначних чисел, як в протоколі, наведеному на фіг.14. Однак при цьому втрачається певний ступінь безпеки, оскільки декодер передає випадкові числа за допомогою інфрачервоного випромінювання. Ця передача, в принципі, може бути перехоплена.

Для шифрування чотиризначного числа, що передається із пристрою дистанційного керування 2026 в приймач-декодер 2020, можна використати безліч інших способів. Однак функція залишку цілочисельного ділення забезпечує для даних цілей достатній ступінь безпеки.

Очевидно, що цей винахід був описаний вище виключно у вигляді прикладу, і можливі різні модифікації в межах даного винаходу.

Кожна особливість, викладена в описі, а також (де це доречно) пункти формули і фігури можуть бути надані незалежно або у відповідному поєднанні.

У вищезазначених варіантах реалізації, яким віддається перевага, певні засоби винаходу, що пропонується, реалізовані з використанням програмного забезпечення. Однак фахівцям, звичайно, зрозуміло,

Fig.2.

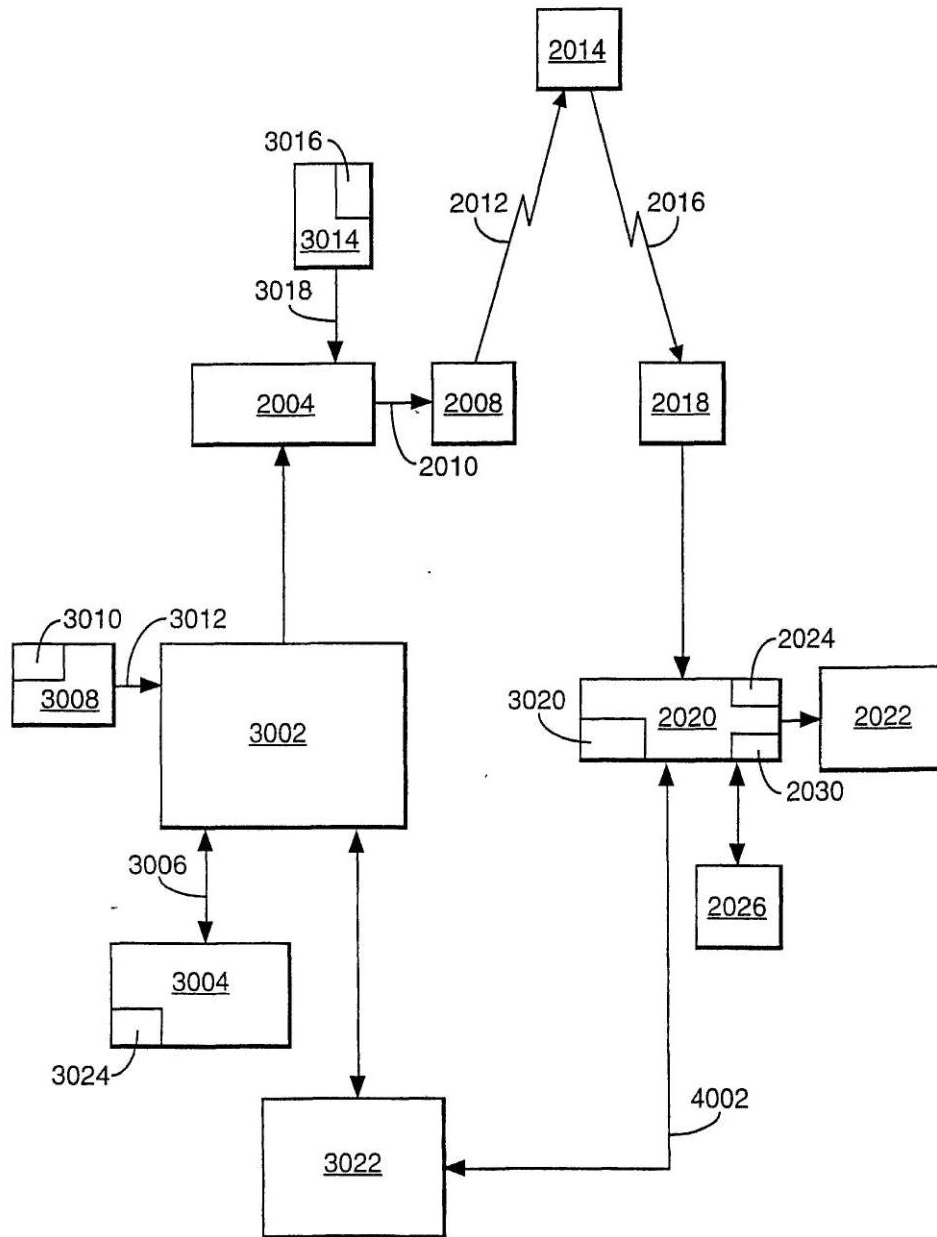


Fig.3.

3066 ІДЕНТИФІКАТОР ТИПУ	3068 ІДЕНТИФІКАТОР РОЗМІРУ	3070 АДРЕСА	3072 ІДЕНТИФІКАТОР ОПЕРАТОРА		
ЗАГОЛОВОК				ВЛАСНЕ ЕММ	ПІДПИС
3060				3062	3064

Fig.4.

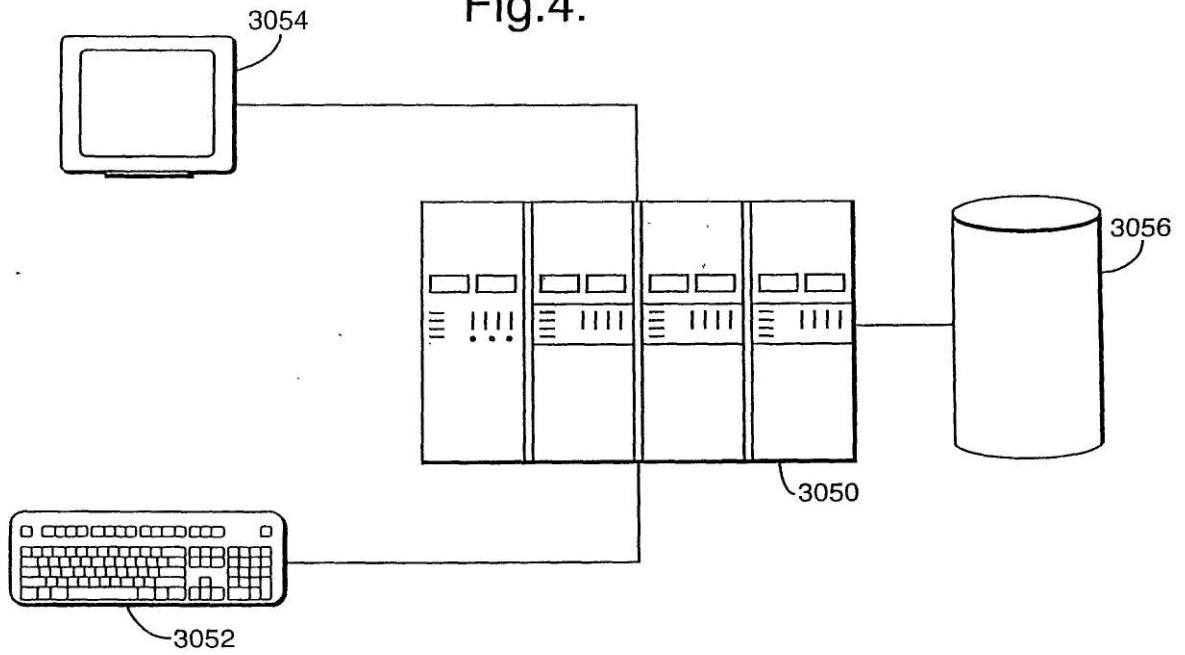


Fig.5.

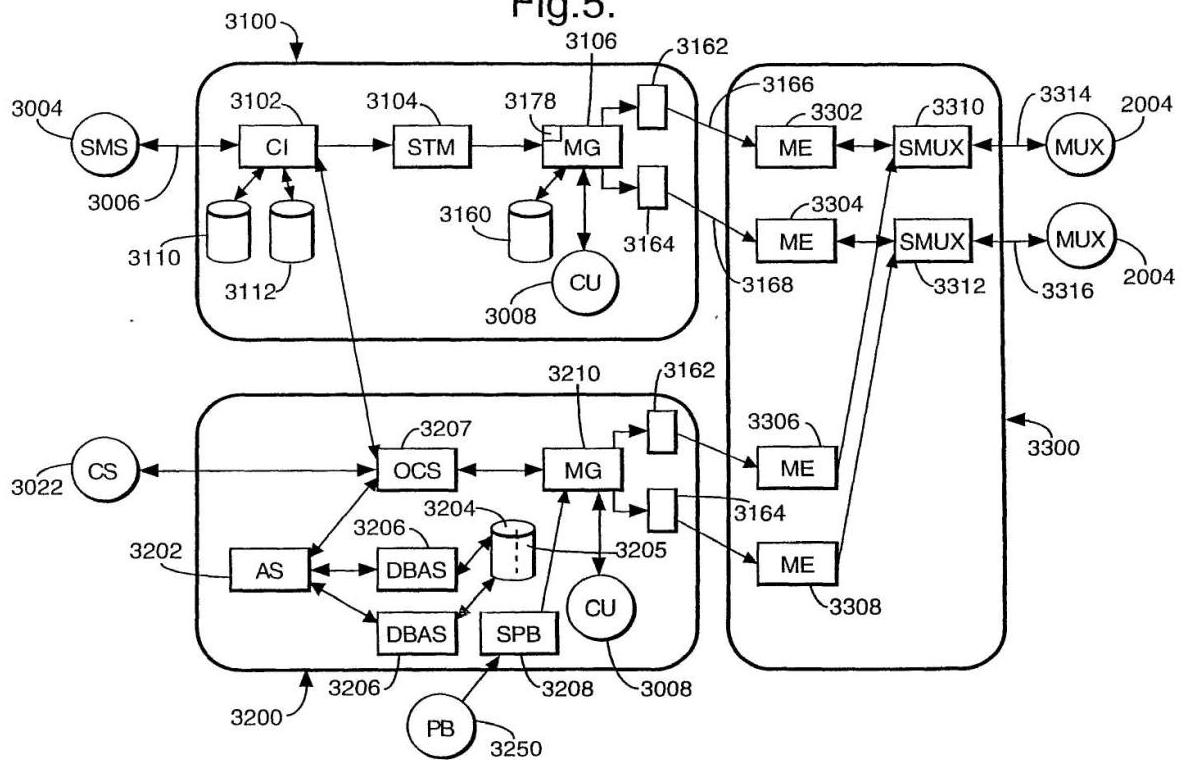


Fig.6.

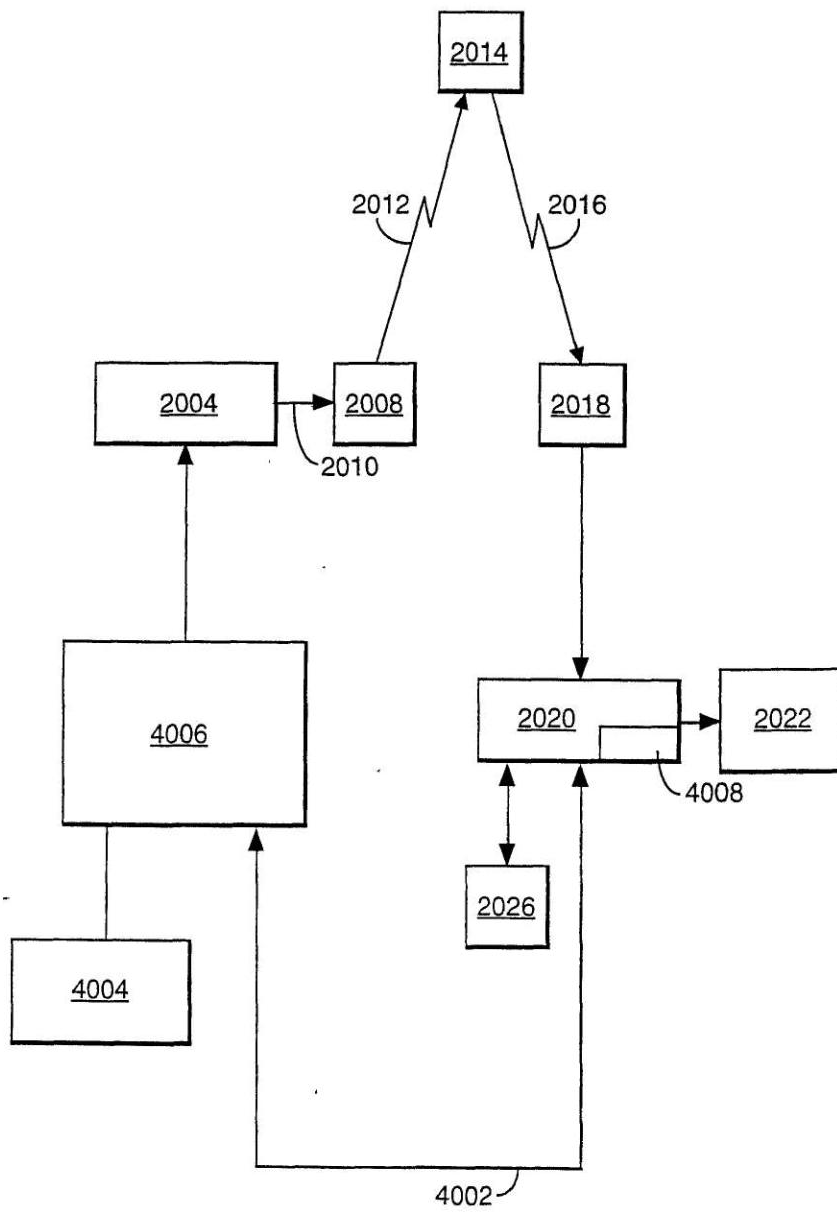


Fig.7.

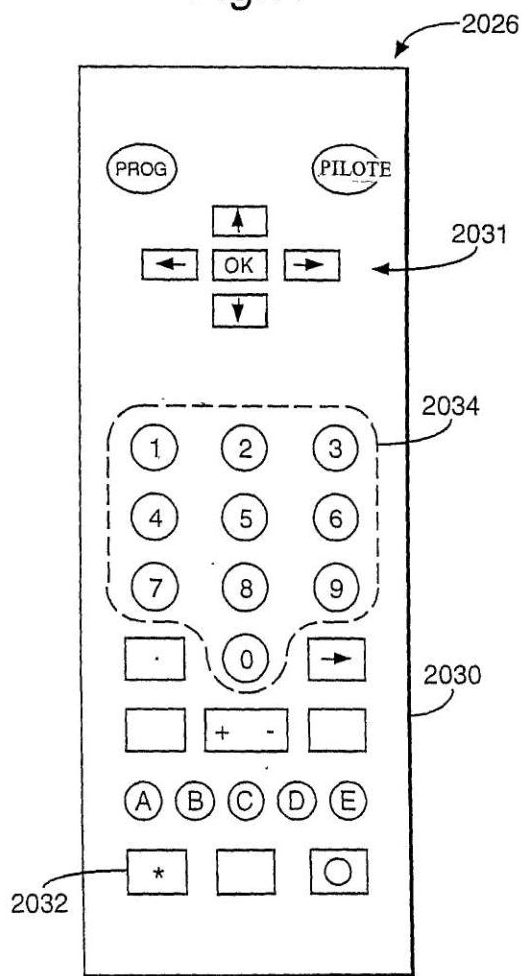


Fig.8.

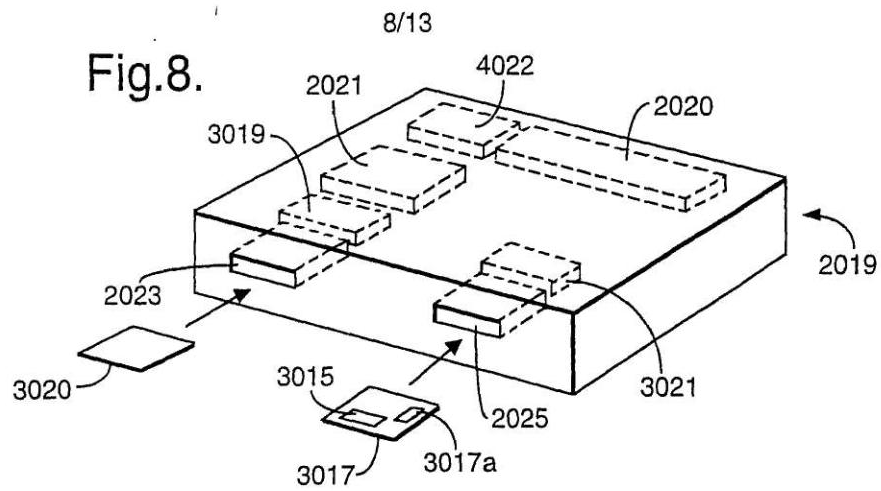


Fig.9.

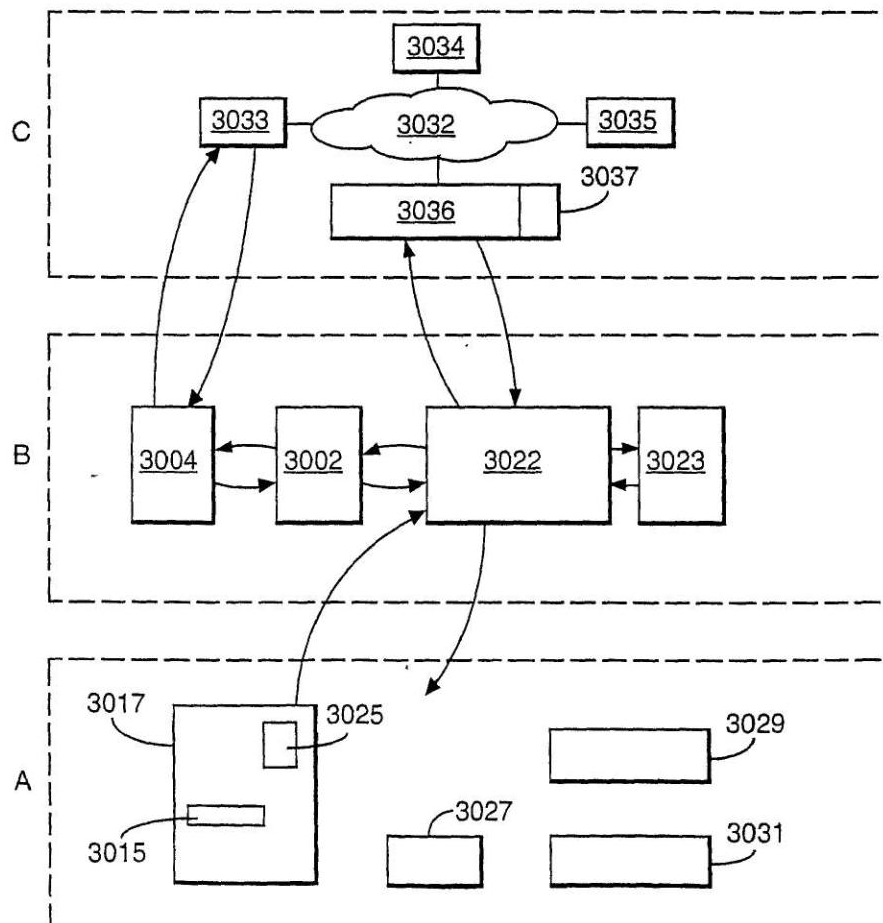


Fig.10.

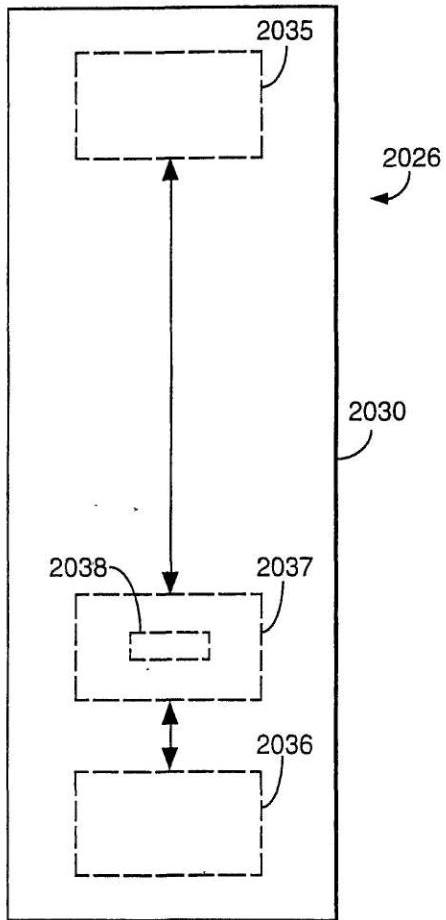


Fig.11.

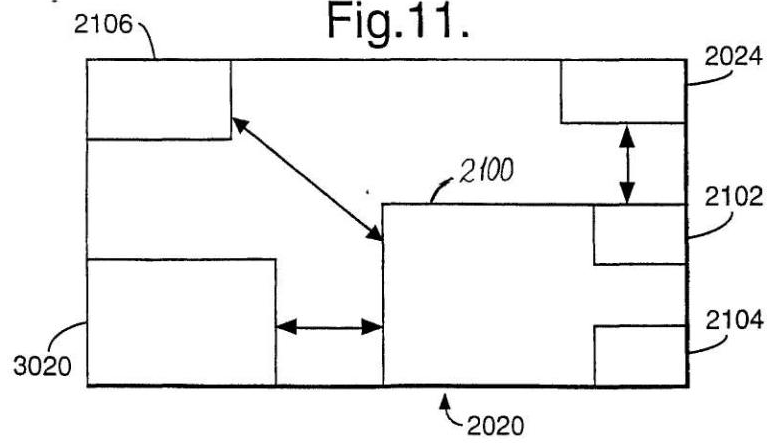


Fig.12.

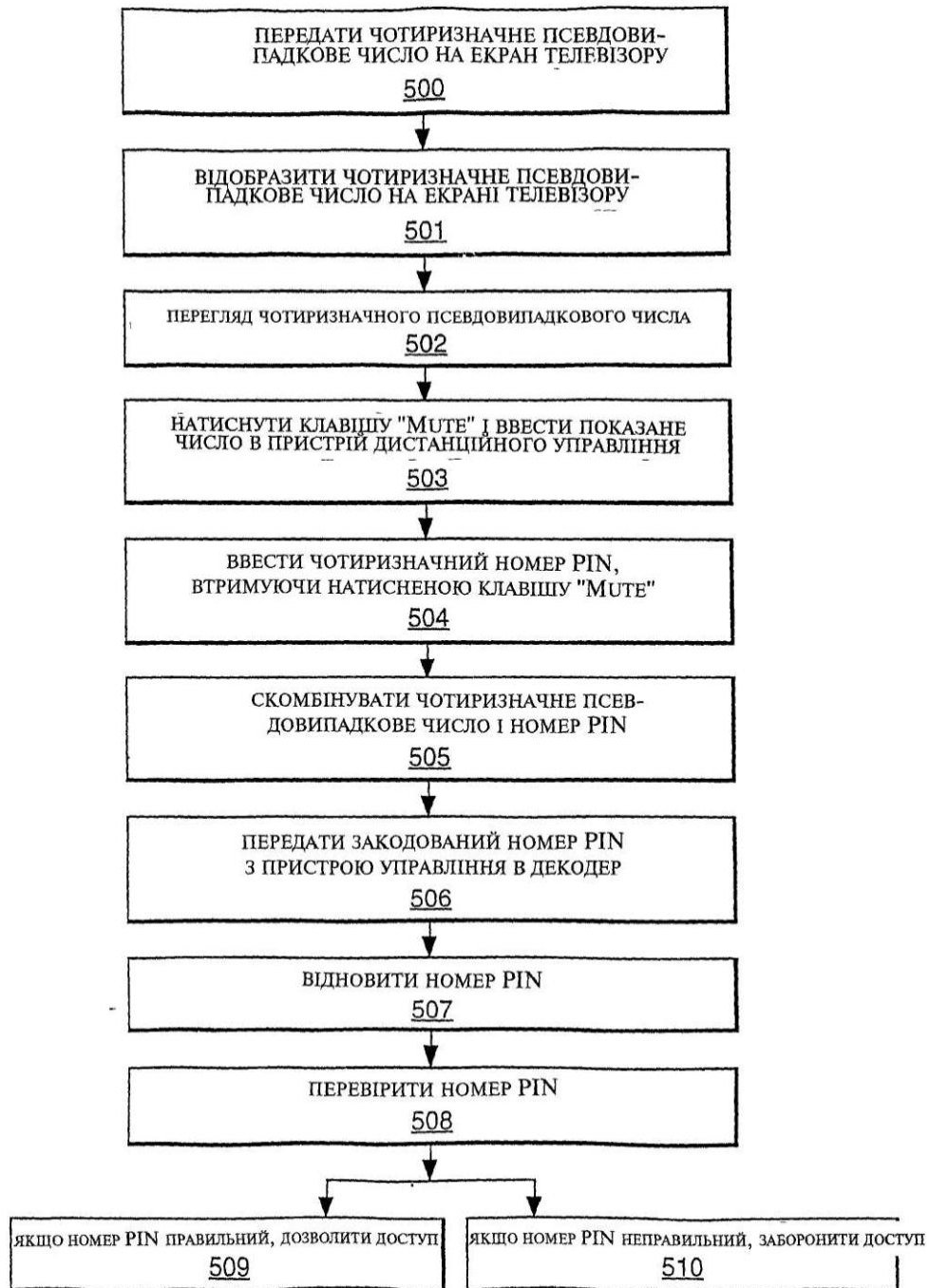


Fig.13.

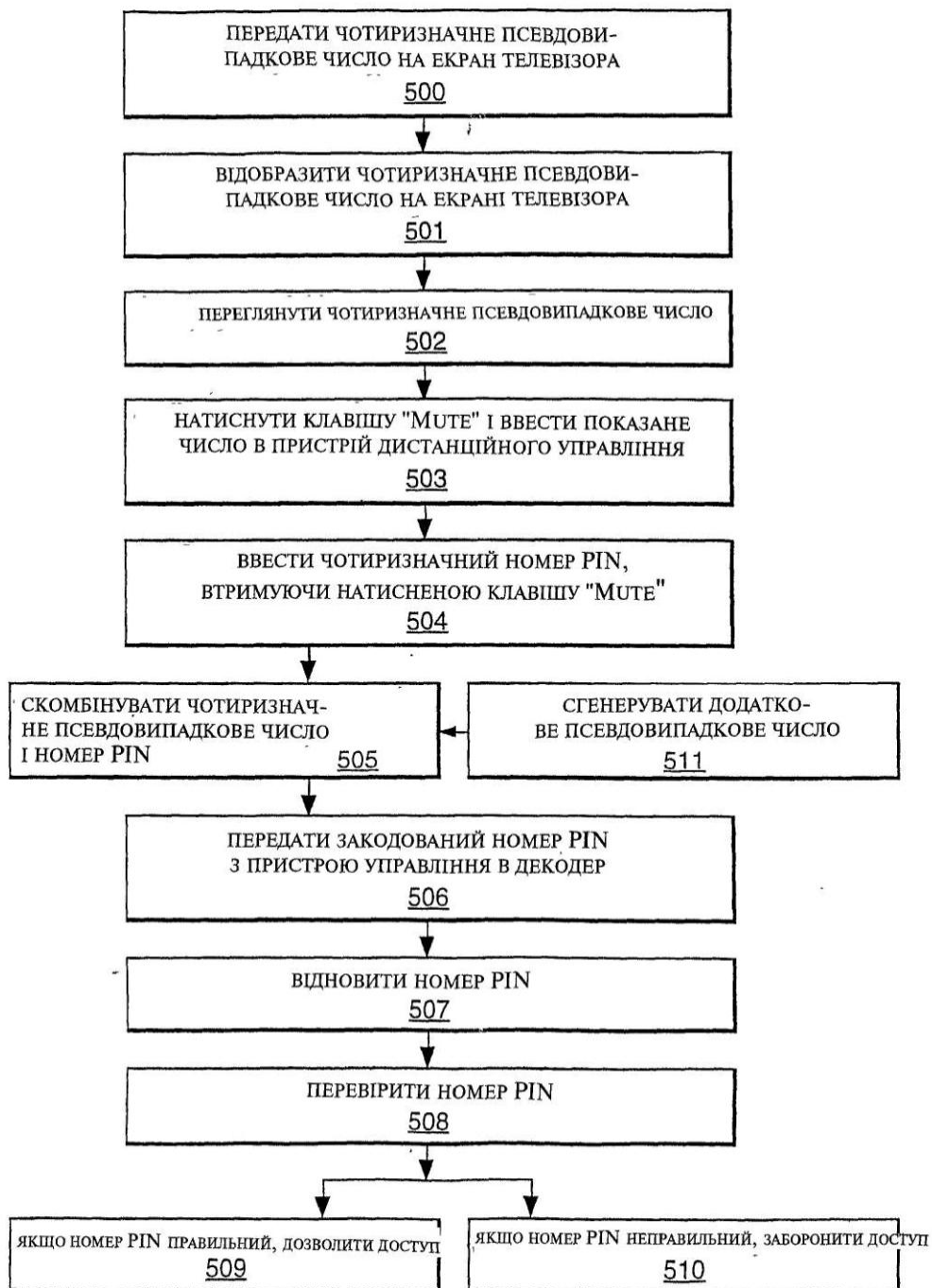


Fig.14.

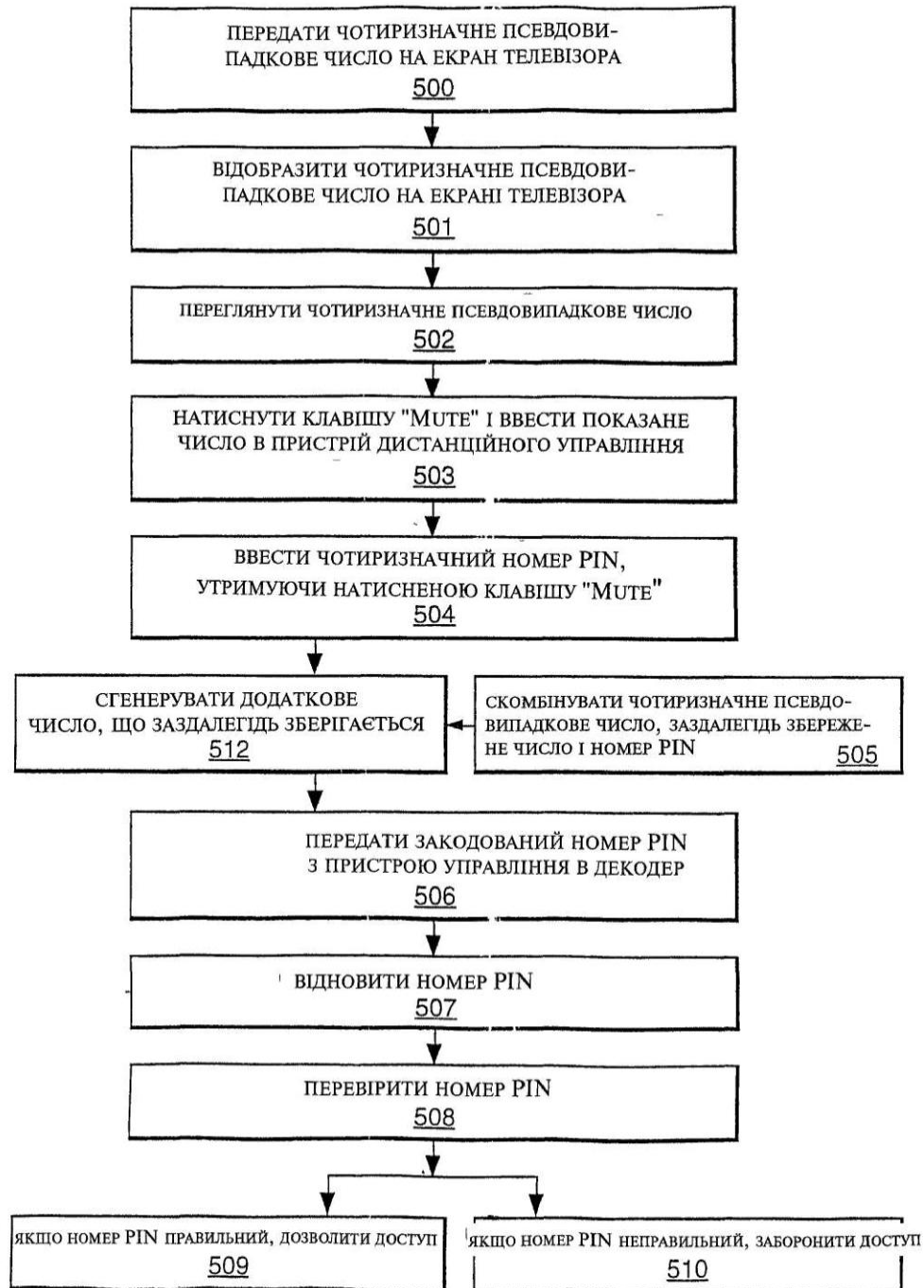


Fig.15.

