

Цей винахід стосується способу і пристрою для забезпечення захищеного передавання цифрових даних між пристроями. Зокрема, цей винахід стосується запобігання незаконному копіюванню і поширенню даних, записаних в цифровому вигляді.

Впровадження цифрових технологій опрацювання аудіовізуальної інформації надало споживачу значні переваги в порівнянні з аналоговими технологіями, особливо в тому, що стосується якості відтворюваних звуку і зображення, а також довговічності носія. Компакт-диск практично замінив традиційні вінілові платівки, і аналогічна ситуація очікується з виходом на ринки мультимедіа і домашніх розваг нових цифрових пристроїв загалом, і особливо - DVD-плеєрів(пристроїв для відтворення DVD-дисків).

Проблема, яка заслуговує особливої уваги, що пов'язана з даними, записаними в цифровій формі, полягає в легкості їх тиражування і, як наслідок, можливостях для «піратства», що з'являються при цьому. Один примірник цифрового запису може бути використаний для створення будь-якої кількості копій без яких-небудь втрат у якості звуку або зображення. Ця проблема стала серйозною, особливо з появою цифрових носіїв, що дозволяють записування, таких як мінідиск і цифрова аудіокасета(DAT), і спричинене існуванням цієї проблеми небажання компаній, які працюють в індустрії розваг, ліцензувати твори, на які розповсюджується дія авторських прав, гальмує вихід на ринок нової інформаційної продукції.

До цього часу найбільш поширеним на практиці вирішенням проблеми несанкціонованого тиражування творів, на які розповсюджується дія авторських прав, було правове, і ряд країн в Європі і в інших частинах світу прийняли "антипіратські" законодавчі акти, для боротьби із все зростаючою кількістю «піратських» фільмів, компакт-дисків тощо, які з'являються на ринку. З цілком очевидних причин правове вирішення є далеко не оптимальним з точки зору недопущення «піратських» дій.

Запропоновані на сьогоднішній день технічні рішення для запобігання несанкціонованому копіюванню і поширенню записаних в цифровій формі даних мають надзвичайно загальний характер, спираючись, наприклад, на ідею використання якої-небудь форми цифрового підтвердження встановлення зв'язку("handshaking") між пристроями в цифровій аудіовізуальній системі, наприклад, між пристроєм для відтворення цифрових даних, або DVD-плеєром, і цифровим записувальним пристроєм, і між DVD-плеєром і цифровим телевізором, щоб перевірити походження пристрою, який приймає дані з DVD-плеєра. Однак такий захист є ефективний лише при тиражуванні, здійснюваному на самому низькому рівні, оскільки сигнал підтвердження зв'язку звичайно ніяк не захищений і може бути легко прочитаний і відтворений, наприклад, для того щоб несанкціонований записувальний пристрій сприймався як санкціонований.

Метою цього винаходу є подолання недоліків, характерних для відомих із рівня техніки методик, і має своєю задачею запропонувати технічне вирішення проблеми несанкціонованого копіювання і відтворення записаних в цифровій формі творів, на які розповсюджується дія авторських прав.

Згідно з першим аспектом цього винаходу пропонується спосіб забезпечення захищеного передавання цифрових даних між пристроями, який включає в себе операції передавання від одного пристрою в автономний захисний модуль ідентифікатора пристрою і перевірки повноважності пристрою, в залежності від значення зазначеного переданого ідентифікатора.

У такому способі для перевірки повноважності певного пристрою, наприклад, в цифровій аудіовізуальній системі, використовується автономний захисний модуль. Наприклад, в системі, в якій дані передаються від DVD-плеєра в цифровий записувальний пристрій, користувач системи міг би мати відповідну смарт-карту для перевірки повноважності записувального пристрою і/або плеєра перед передаванням яких-небудь даних. Таким чином, шляхом використання захисного модуля для перевірки повноважності пристроїв система може бути забезпечена додатковим рівнем захисту.

Фактично застосування автономного захисного модуля дозволяє отримати надзвичайно індивідуалізовану цифрову аудіовізуальну систему. Наприклад, зазначений захисний модуль може дозволяти передавати дані від DVD-плеєра в цифровий телевізор тільки в тому випадку, якщо і плеєр, і телевізор будуть визнані повноважними зазначеним захисним модулем, дозволяючи таким чином переглядати цифрові дані тільки на особистому телевізорі користувача.

Використання захисного модуля для перевірки повноважності з'єднаних пристроїв забезпечує також перевагу, яка полягає в тому, що перевірку повноважності пристроїв можна зробити незалежно від каналу зв'язку, який з'єднує самі пристрої. Таким чином, у разі перехоплення даних, які передаються по цьому каналу зв'язку, третьою особою вона не зможе отримати ідентифікатори пристроїв, оскільки вони передаються не між самими пристроями, а від кожного із пристроїв в захисний модуль.

Такі захисні модулі можуть бути виконані в будь-якій придатній формі, в залежності від необхідних фізичних розмірів і характеристик. Наприклад, захисний модуль може бути знімним, наприклад, таким, що встановлюється з можливістю виймання в гніздо, передбачене в пристрої або в окремому модулі, який підключається до такого пристрою. У певних випадках може використовуватися смарт-карта, аналогічна банківській картці(як захисний модуль або як частина захисного модуля), але однаковою мірою можливі і інші формати, такі як карти типу PCMCIA. Таким чином, захисний модуль можна легко замінювати, з метою оновлення прав, які надаються захисним модулем, наприклад, щоб позбавити певні пристрої повноважності в тому випадку, коли постачальнику системи стане відомо про клонування цих пристроїв.

Зазначений ідентифікатор пристрою може приймати будь-яку зручну форму. Наприклад, цей ідентифікатор може бути відкритим ключем, асоційованим із відповідним пристроєм.

Захисний модуль може виконувати перевірку повноважності пристрою шляхом порівняння зазначеного переданого ідентифікатора з щонайменше одним збереженим ідентифікатором. Збережені ідентифікатори можуть зберігатися в пам'яті захисного модуля. Ці ідентифікатори можуть зберігатися у вигляді списку, і для перевірки повноважності пристрою зазначений прийнятий ідентифікатор порівнюється із зазначеними

ідентифікаторами, які входять в список. Таким чином може бути забезпечена швидка і ефективна перевірка повноважності пристрою.

Кожний збережений ідентифікатор може бути асоційований або з певним повноважним пристроєм, або з певним неповноважним пристроєм. Приймаючи зазначений ідентифікатор, захисний модуль може порівняти прийнятий ідентифікатор із збереженими ідентифікаторами, асоційованими з неповноважними пристроями, і/або із збереженими ідентифікаторами, асоційованими з повноважними пристроями.

Таким чином, в захисному модулі може зберігатися щонайменше один список - "відмовний список", для формування "чорного списку" пристроїв, які не відповідають умовам надання прав доступу, або "санкціонуючий список", для обмеження передавання даних таким чином, що передавання даних можливе лише між заздалегідь зареєстрованими пристроями. Ідентифікатори пристроїв, навмисно опубліковані третіми сторонами, наприклад, в Internet, можуть бути додані в зазначений відмовний список при періодичному оновленні захисного модуля, щоб запобігти передаванню даних в ці пристрої або з них. У той же час шляхом використання санкціонуючого списку також можна запобігти застосуванню ідентифікаторів пристроїв, навмисно опублікованих в Internet, оскільки ці ідентифікатори не будуть дійсні ніде, крім, наприклад, домашньої мережі.

Відповідно, швидше за все санкціонуючий список буде набагато коротшим, ніж відмовний список, дозволяючи таким чином зекономити простір в пам'яті, і, швидше усього, буде потребувати менш частого оновлення. Таким чином, згідно із другим аспектом цього винаходу пропонується спосіб забезпечення захищеного передавання цифрових даних між пристроями, який включає в себе операції порівняння певного ідентифікатора, переданого від одного пристрою, з щонайменше одним збереженим ідентифікатором, причому кожний збережений ідентифікатор є асоційований з відповідним повноважним пристроєм, і визнання цього пристрою повноважним, якщо зазначений переданий ідентифікатор є ідентичний одному із зазначених збережених ідентифікаторів.

У переважному варіанті здійснення зазначений щонайменше один збережений ідентифікатор зберігається в автономному захисному модулі.

Зазначений переданий ідентифікатор може порівнюватися з ідентифікаторами, які асоціюються з повноважними пристроями у відповідності зі значенням певного прапора. Прапор може зберігатися в зазначеному захисному модулі або може передаватися в зазначений захисний модуль зазначеним пристроєм.

Наприклад, захисний модуль може порівнювати прийнятий ідентифікатор із збереженими ідентифікаторами, асоційованими з неповноважними пристроями, якщо зазначений прапор має певне перше значення, і порівнювати прийнятий ідентифікатор із збереженими ідентифікаторами, асоційованими з повноважними пристроями, якщо зазначений прапор має певне друге значення.

Значення такого прапора може встановлюватися відповідно до прав, наданих даному користувачу. Наприклад, прапор може бути встановлений в перше значення у разі певного магазину, в якому застосовуються багато різних пристроїв, і значення прапора встановлюють таким, щоб прийнятий ідентифікатор порівнювався із збереженими ідентифікаторами, асоційованими лише з неповноважними пристроями. Прапор може бути встановлений у друге значення для користувача домашньої системи, де використовується лише невелика кількість пристроїв, і значення прапора в цьому випадку встановлюють таким, щоб прийнятий ідентифікатор порівнювався із збереженими ідентифікаторами, асоційованими лише з повноважними пристроями.

У одному з варіантів здійснення цього винаходу захисний модуль може порівнювати зазначений прийнятий ідентифікатор із збереженими ідентифікаторами, асоційованими з неповноважними пристроями, коли зазначений прапор має значення "0", і порівнювати зазначений прийнятий ідентифікатор як із збереженими ідентифікаторами, асоційованими з неповноважними пристроями, так і із збереженими ідентифікаторами, асоційованими з повноважними пристроями, коли зазначений прапор має значення "1".

У переважному варіанті здійснення цього винаходу для перевірки повноважності пристрою між зазначеними пристроєм і захисним модулем передаються сертифікати.

Використання системи сертифікатів для перевірки повноважності пристрою може забезпечити захищене передавання зазначеного ідентифікатора із зазначеного пристрою в захисний модуль. Таким чином, зазначений ідентифікатор пристрою може бути переданий в захисний модуль в зашифрованому сертифікаті, так що можна буде уникнути проблем, пов'язаних з передаванням ідентифікаторів "відкритим текстом"(незашифрованими).

Зазначений сертифікат може забезпечуватися підписом, наприклад, із використанням секретного ключа, такого як секретний ключ виготівника зазначеного пристрою, щоб забезпечити можливість перевірки автентичності переданого сертифіката. Таким чином, якщо захисний модуль визначить, що дані, які розміщені в сертифікаті, і його підпис не відповідають один одному, то сертифікат може бути відкинтий.

Еквівалентний зазначеному секретному ключу ключ може бути переданий в захисний модуль в сертифікаті, зашифрованому секретним ключем системи, при цьому відкритий ключ системи зберігається як в захисному модулі, так і в самому пристрої.

Зазначений зашифрований сертифікат переважно додатково зашифровується зазначеним пристроєм із використанням відкритого ключа зазначеного захисного модуля і передається в зазначений захисний модуль. Зазначений зашифрований сертифікат може бути потім дешифрований захисним модулем, спочатку з використанням секретного ключа захисного модуля, а потім із використанням зазначеного еквівалентного ключа, щоб забезпечити можливість витягання зазначеного ідентифікатора пристрою із зазначеного зашифрованого сертифіката.

Зазначений відкритий ключ захисного модуля може бути переданий захисним модулем зазначеному пристрою в певному сертифікаті. Цей сертифікат, який включає в себе відкритий ключ захисного модуля, може бути зашифрований з використанням секретного ключа, наприклад, виготівника захисного модуля. Щоб зробити можливою перевірку автентичності переданого сертифіката, цей сертифікат також може забезпечуватися підписом, із використанням зазначеного секретного ключа. Еквівалентний цьому секретному ключу ключ може бути переданий зазначеному пристрою в певному сертифікаті, зашифрованому з використанням зазначеного секретного ключа системи, при цьому відкритий ключ системи зберігається і в захисному модулі, і в самому пристрої.

Перед шифруванням зазначений сертифікат, який включає в себе ідентифікатор пристрою, може бути підданий рандомізації, яка може бути обернена захисним модулем після дешифрування зазначеного сертифіката. Таким чином може бути підвищена захищеність при передаванні ідентифікатора пристрою від зазначеного пристрою в захисний модуль.

Додатково до перевірки певного пристрою захисний модуль може передавати в цей пристрій інформацію, для того щоб, наприклад, забезпечити зазначеному пристрою можливість опрацювання цифрових даних, які приймаються від іншого пристрою. Таким чином, переважним було б організувати між зазначеним пристроєм і захисним модулем захищений канал зв'язку.

У одному переважному варіанті здійснення цього винаходу зазначеним пристроєм генерується певне випадкове число, причому це випадкове число і зазначений сертифікат, який містить ідентифікатор пристрою, зашифровуються зазначеним пристроєм із використанням відкритого ключа захисного модуля і передаються в захисний модуль. Зазначені зашифровані випадкове число і сертифікат можуть дешифруватися захисним модулем із використанням секретного ключа захисного модуля для отримання зазначеного випадкового числа і забезпечення можливості витягання із зазначеного зашифрованого сертифіката ідентифікатора пристрою.

Витягнуте випадкове число може бути потім збережене в захисному модулі, так що згодом дані, які передаються між захисним модулем і зазначеним пристроєм, можуть бути зашифровані і дешифровані з використанням цього випадкового числа в зазначених захисному модулі і пристрої, забезпечуючи таким чином захищений канал зв'язку між зазначеними пристроєм і захисним модулем.

Таким чином, згідно із третім аспектом цього винаходу пропонується спосіб забезпечення захищеного передавання цифрових даних між певним пристроєм і захисним модулем, який включає в себе операції передавання в захисний модуль певного випадкового числа і ідентифікатора зазначеного пристрою, зашифрованих із використанням відкритого ключа зазначеного захисного модуля, дешифрування захисним модулем зазначених випадкового числа і ідентифікатора пристрою з використанням секретного ключа зазначеного захисного модуля, перевірки повноважності зазначеного пристрою з використанням зазначеного ідентифікатора пристрою, і, після визнання пристрою повноважним, використання зазначеного випадкового числа для шифрування і дешифрування даних, які передаються між зазначеними захисним модулем і пристроєм.

У переважному варіанті здійснення зазначений ідентифікатор пристрою включається в певний сертифікат, який зашифровується з використанням зазначеного відкритого ключа захисного модуля.

Перед шифруванням зазначене випадкове число може бути піддане рандомізації зазначеним пристроєм, а після дешифрування зазначеного випадкового числа ця рандомізація може бути обернена захисним модулем.

У альтернативному варіанті зазначені випадкове число і сертифікат, який включає в себе ідентифікатор пристрою, можуть бути піддані рандомізації зазначеним пристроєм перед шифруванням, а після дешифрування зазначених випадкового числа і сертифіката ця рандомізація може бути обернена захисним модулем.

Для того щоб підвищити захищеність каналу зв'язку між зазначеними пристроєм і захисним модулем, захисний модуль може передавати в зазначений пристрій певний випадковий ключ, згенерований в захисному модулі і зашифрований з використанням зазначеного випадкового числа, при цьому зазначений пристрій дешифрує зазначений ключ із використанням зазначеного випадкового числа і після цього використовує зазначений ключ для шифрування даних, які передаються в захисний модуль.

Додатково до перевірки повноважності пристрою і для забезпечення безпеки при обмінюванні даними між зазначеними пристроєм і захисним модулем, захисний модуль може бути виконаний з можливістю надання прав доступу для доступу до даних, які приймаються зазначеним пристроєм.

Наприклад, зазначений пристрій може передавати в захисний модуль зашифроване повідомлення керування правами (ECM - Entitlement Control Message), яке включає в себе керуюче слово для дескремблювання даних, при цьому зазначене зашифроване повідомлення ECM додатково зашифровується зазначеним пристроєм із використанням зазначеного ключа. Таким чином, повідомлення ECM, які передаються між певним пристроєм і захисним модулем, зашифровуються двічі, причому один із відповідних ключів шифрування генерується захисним модулем і тому є унікальним для даних пристрою і захисного модуля. Завдяки цьому може бути істотно посилений захист від незаконного копіювання і поширення повідомлень ECM.

Захисний модуль може дешифрувати зашифроване ECM, витягувати з нього зазначене керуюче слово і передавати це керуюче слово, зашифроване з використанням зазначеного ключа, в зазначений пристрій.

Завдяки цьому певному пристрою, такому як цифровий телевізор, може бути забезпечена можливість дескремблювання скремблених даних, які приймаються від DVD-плеєра. Більш того зазначене керуюче слово може завжди передаватися в зазначений пристрій в зашифрованій формі, причому зазначене шифрування здійснюється з використанням певного ключа, заздалегідь переданого в

зазначений пристрій після встановлення повноважності пристрою. Відповідно, нема потреби в зберіганні додаткових відкритих/секретних ключів для шифрування і дешифрування керуючих слів, або для асоціювання зазначеного пристрою із захисним модулем(або навпаки).

У альтернативному варіанті здійснення зазначений пристрій може передавати в захисний модуль зашифроване розширене повідомлення керування правами (XECM - extended ECM), яке включає в себе розширену керуючу інформацію (XCM - extended Control Management Information), або права доступу для доступу до даних, причому зазначений пристрій додатково зашифровує зашифроване повідомлення XECM із використанням зазначеного ключа. Захисний модуль може дешифрувати зашифроване повідомлення XECM, модифікувати права доступу, які містяться в повідомленні XECM, зашифровувати модифіковане повідомлення XECM і передавати в зазначений пристрій зашифроване повідомлення XECM, додатково зашифроване з використанням зазначеного ключа.

Таким чином, захисний модуль може модифікувати права доступу, які надаються зазначеному пристрою в повідомленні XECM. Наприклад, якщо цим пристроєм є цифровий записувальний пристрій, ці права можуть включати в себе заборону на який би то не було подальший перезапис збережених даних, кількість дозволених відтворень збережених даних, дату закінчення терміну, протягом якого дозволяється відтворення, тощо.

Для того, щоб зробити можливим більш ефективне функціонування зазначених пристроїв, між ними бажано організувати захищений канал зв'язку, або канал зв'язку з шифруванням. Захищене з'єднання між пристроями може бути використане для забезпечення можливості вільного передавання між пристроями інформації, необхідного для створення або відтворення запису. На жаль, неузгодженість дій виготівника DVD-плеєра і виготівника записувального обладнання, відповідального за записувальний пристрій, може призвести до виникнення ряду проблем в тому, що стосується забезпечення ключами шифрування для цієї мети.

Наприклад, виготівник плеєра може недостатньо довіряти надійності системи безпеки на заводі, який виготовляє записувальний пристрій, для того щоб довірити його виробнику, наприклад, секретний ключ симетричного алгоритму, необхідний записувальному пристрою для дешифрування повідомлень, зашифрованих із використанням еквівалентного ключа, який має DVD-плеєр.

Крім того, внаслідок розділення сфер діяльності може виявитися непрактичним покладатися на те, що записувальний пристрій будуть посилати адміністратору системи мовлення для індивідуалізації з використанням відповідних ключів. Враховуючи цю обставину, необхідно знайти рішення, яке допускало б найбільшу незалежність в функціонуванні плеєра і записувального пристрою.

Для вирішення таких проблем відповідно до переважного варіанту здійснення цього винаходу дані передаються між першим і другим пристроями, і, після перевірки захисним модулем повноважності кожного із пристроїв, захисний модуль передає в перший пристрій певний випадковий ключ, згенерований в захисному модулі і зашифрований з використанням випадкового числа, згенерованого першим пристроєм, причому перший пристрій дешифрує цей ключ із використанням зазначеного згенерованого ним випадкового числа, і передає у другий пристрій зазначений ключ, зашифрований з використанням випадкового числа, згенерованого другим пристроєм, причому цей другий пристрій дешифрує цей ключ із використанням зазначеного згенерованого ним випадкового числа, і цей ключ потім використовується для шифрування даних, які передаються в захисний модуль зазначеними пристроями, і даних, які передаються між цими пристроями.

Відповідно, згідно з четвертим аспектом цього винаходу пропонується спосіб забезпечення захищеного передавання цифрових даних між пристроями, який включає в себе операції надання захисного модуля, генерування в цьому захисному модулі певного випадкового ключа(SK) і шифрування даних, які передаються між зазначеними пристроями, з використанням зазначеного випадкового ключа.

За допомогою цього способу генерування ключа шифрування для забезпечення безпечного обміну даними між пристроями здійснюється захисним модулем, який бере участь в обміні даними із пристроями, так що генерування ключа здійснюється автономно від зазначених пристроїв.

Такий спосіб може забезпечити надійну, гнучку і здатну до розширювання систему, незалежну від типу інтерфейсів пристроїв, яка забезпечує захищене передавання цифрових даних між пристроями. Ця система може бути базована на застосуванні смарт-карти для генерування сеансового ключа, і тому бути недорогою і такою, що дозволяє вживати оперативні заходи проти дій «піратів» завдяки легкості оновлення смарт-карт, особливо якщо відповідальність за постійну підтримку належного рівня захищеності може бути покладена на постачальника смарт-карт, який спеціалізується на цьому, а не на виготівників пристроїв.

Захисний модуль може передавати в кожний пристрій зазначений ключ, зашифрований з використанням певного випадкового числа, згенерованого даним пристроєм, причому відповідний пристрій дешифрує зазначений ключ із використанням відповідного випадкового числа.

Кожний пристрій може передавати в захисний модуль відповідне випадкове число, зашифроване з використанням відкритого ключа зазначеного захисного модуля. Це зашифроване випадкове число може потім дешифруватися захисним модулем із використанням секретного ключа захисного модуля для отримання зазначеного випадкового числа. Перед шифруванням кожне випадкове число може бути піддане відповідним пристроєм рандомізації, яка обертається захисним модулем після дешифрування даного випадкового числа. У переважному варіанті здійснення захисний модуль перевіряє повноважність кожного пристрою перед передаванням зазначеного ключа в кожний пристрій. Для забезпечення можливості здійснення такої перевірки повноважності в переважному варіанті здійснення кожний пристрій передає свій певний ідентифікатор в захисний модуль для перевірки захисним модулем повноважності даного пристрою.

Захисний модуль може періодично змінювати зазначений ключ. Цей ключ може оновлюватися, наприклад, щогодини, або після передавання між пристроями певної наперед заданої кількості пакетів даних. Це може ще більше підвищити рівень безпеки передавання даних. У альтернативному варіанті здійснення зазначений ключ може змінюватися захисним модулем довільно, наприклад, після ввімкнення пристрою, устанавлення диска, перемикання даного пристрою користувачем на інший канал, встановлення з'єднання з даним захисним модулем тощо.

Один із переважних варіантів здійснення цього винаходу є реалізований застосовно до системи домашньої мережі, де зазначені пристрої відповідають першому і другому побутовим електронним пристроям, виконаним із можливістю обміну між собою даними через який-небудь канал зв'язку. Цей канал зв'язку між зазначеними двома пристроями може приймати одну з численних форм, наприклад, може бути радіоканалом, телефонним або інфрачервоним каналом. Однак в переважному варіанті здійснення зазначений канал зв'язку реалізовується шляхом підключення зазначених першого і другого пристроїв до певної шини, наприклад, до шини IEEE 1394.

Перший пристрій може передавати у другий пристрій скрембльовані аудіо- і/або відеодані і зашифроване повідомлення керування правами(ЕСМ), яке включає в себе керуюче слово для дескремблювання зазначених даних, причому зазначені дані і зазначене зашифроване ЕСМ зашифровуються першим пристроєм із використанням зазначеного ключа.

Другий пристрій може дешифрувати зазначені дані і зашифроване ЕСМ, використовуючи зазначений ключ, відділяти зашифроване ЕСМ від зазначених даних і передавати в захисний модуль зашифроване повідомлення ЕСМ, повторно зашифроване з використанням зазначеного ключа. Захисний модуль може дешифрувати зашифроване повідомлення ЕСМ, витягувати з цього повідомлення ЕСМ керуюче слово і передавати у другий пристрій зазначене керуюче слово, зашифроване з використанням зазначеного ключа. У цьому варіанті здійснення цього винаходу зазначеним першим пристроєм може бути DVD-плеєр, і зазначеним другим пристроєм може бути цифровий телевізор.

Крім того, захисний модуль може модифікувати зазначене повідомлення ЕСМ і передавати у другий пристрій модифіковане повідомлення ЕСМ, зашифроване з використанням зазначеного ключа. У цьому варіанті здійснення цього винаходу зазначеним першим пристроєм може бути DVD-плеєр, і зазначеним другим пристроєм може бути цифровий записувальний пристрій.

Згідно з п'ятим аспектом цього винаходу пропонується пристрій для забезпечення захищеного передавання цифрових даних між пристроями, який включає в себе захисний модуль, що в свою чергу включає в себе засіб для приймання ідентифікатора певного пристрою і засіб для перевірки повноважності пристрою, в залежності від значення прийнятого ідентифікатора.

Згідно з сьомим аспектом цього винаходу пропонується захисний модуль для забезпечення захищеного передавання цифрових даних між пристроями, який виконаний з можливістю приймання ідентифікатора певного пристрою і перевірки повноважності пристрою в залежності від значення прийнятого ідентифікатора.

Згідно з шостим аспектом цього винаходу пропонується пристрій для забезпечення захищеного передавання цифрових даних між пристроями, який включає в себе засіб для зберігання щонайменше одного ідентифікатора, причому кожний збережений ідентифікатор є асоційований з відповідним повноважним пристроєм, засіб для порівняння ідентифікатора певного пристрою із зазначеним щонайменше одним збереженим ідентифікатором, і засіб для визнання цього пристрою повноважним у випадку, якщо зазначений ідентифікатор пристрою ідентичний одному із зазначених збережених ідентифікаторів.

Згідно з суміжним аспектом цього винаходу пропонується захисний модуль для забезпечення захищеного передавання цифрових даних між пристроями, який виконаний з можливістю зберігання щонайменше одного ідентифікатора, причому кожний збережений ідентифікатор є асоційований з відповідним повноважним пристроєм, порівняння ідентифікатора певного пристрою із зазначеним щонайменше одним збереженим ідентифікатором і визнання цього пристрою повноважним у випадку, якщо зазначений ідентифікатор пристрою є ідентичний одному із зазначених збережених ідентифікаторів.

Згідно з сьомим аспектом цього винаходу пропонується система для забезпечення захищеного передавання даних між певним пристроєм і захисним модулем, причому зазначений пристрій включає в себе засіб для передавання в захисний модуль певного випадкового числа і ідентифікатора даного пристрою, зашифрованого з використанням відкритого ключа зазначеного захисного модуля, і захисний модуль включає в себе засіб для дешифрування зазначених випадкового числа і ідентифікатора пристрою з використанням секретного ключа захисного модуля, засіб для перевірки повноважності зазначеного пристрою з використанням зазначеного ідентифікатора пристрою, і засіб для використання зазначеного випадкового числа для шифрування і дешифрування даних, які передаються між зазначеними захисним модулем і пристроєм.

Згідно з суміжним аспектом цього винаходу пропонується захисний модуль, який виконаний з можливістю приймання певного випадкового числа і ідентифікатора певного пристрою, зашифрованого з використанням відкритого ключа даного захисного модуля, дешифрування зазначених випадкового числа і ідентифікатора пристрою з використанням секретного ключа даного захисного модуля, перевірки повноважності зазначеного пристрою з використанням зазначеного ідентифікатора пристрою і використання зазначеного випадкового числа, після визнання пристрою повноважним, для шифрування і дешифрування даних, які передається між зазначеними захисним модулем і пристроєм.

Згідно з восьмим аспектом цього винаходу пропонується пристрій для забезпечення захищеного передавання цифрових даних між пристроями, який включає в себе зазначені пристрої і захисний модуль,

який включає в себе засіб для генерування випадкового ключа і засіб для передавання зазначеного випадкового ключа в зазначені пристрої, кожен з яких є виконаний з можливістю шифрування даних, які передаються між цими пристроями, з використанням зазначеного випадкового ключа.

Згідно з суміжним аспектом цього винаходу пропонується захисний модуль для забезпечення захищеного передавання цифрових даних між пристроями, який виконаний з можливістю генерування випадкового ключа(SK) для шифрування даних, які передаються між зазначеними пристроями, і передавання зазначеного випадкового ключа в зазначені пристрої.

Хоч цей винахід був описаний з посиланнями на перший і другий пристрої, потрібно розуміти, що цей же принцип може бути використаний для організації ланцюжка з'єднань між кількома такими пристроями.

До числа придатних для використання в цьому винаході алгоритмів із секретним і відкритим ключами відносяться, наприклад, RSA, алгоритм Фіата-Шаміра(Fiat-Shamir) або алгоритм Діффі-Хеллмана(Diffie-Hellman), а до числа придатних алгоритмів шифрування з симетричним ключем відносяться, наприклад, алгоритми типу DES. Однак, якщо супротивне не зумовлене контекстом або не обумовлене прямо, не робиться принципових відмінностей між ключами, асоційованими з симетричними алгоритмами, і ключами, асоційованими з алгоритмами шифрування з відкритим і секретним ключами.

Терміни "скрембльований" і "зашифрований", а також "керуюче слово" і "ключ" використані в різних місцях цього тексту з міркувань літературності мови. Однак очевидно, що не треба робити ніяких принципових відмінностей між термінами "скрембльовані дані" і "зашифровані дані", або між термінами "керуюче слово" і "ключ".

Крім того, з міркувань літературності мови в різних місцях цього тексту використані терміни "зашифрований" і "забезпечений підписом", "дешифрований" і "перевірений". Однак очевидно, що не треба робити ніяких принципових відмінностей між термінами "зашифровані дані" і "забезпечені підписом дані", або між термінами "дешифровані дані" і "перевірені дані".

Аналогічно, термін "еквівалентний ключ" використовується для позначення ключа, придатного для дешифрування даних, зашифрованих із використанням раніше зазначеного ключа, або навпаки.

Описані вище ознаки, які відносяться до аспектів цього винаходу, що стосуються способів, можуть бути також застосовані до аспектів, що стосуються пристроїв, і навпаки.

Переважні особливості цього винаходу будуть описані нижче на виключно ілюстративному прикладі, з посиланнями на прикладені малюнки, на яких:

- фіг.1 - елементи цифрової аудіовізуальної системи;
- фіг.2 - розподіл сертифікатів в цифровій аудіовізуальній системі;
- фіг.3 - з'єднання захисного модуля з пристроєм;
- фіг.4 - з'єднання захисного модуля з двома пристроями;
- фіг.5 - операції, які виконуються при перевірці повноважності пристрою захисним модулем і подальшому забезпеченні захищеного зв'язку між пристроєм і захисним модулем;
- фіг.6 - операції, які виконуються при організації захищеного каналу зв'язку між пристроєм і захисним модулем;
- фіг.7 - дескремблювання даних, які приймаються пристроєм;
- фіг.8 - операції, які виконуються при організації захищеного зв'язку між пристроями;
- фіг.9 - передавання даних між двома пристроями по захищеному каналу зв'язку;
- фіг.10 - операції, які виконуються при організації захищеного каналу зв'язку між DVD-плеєром і цифровим телевізором, і подальші операції, які виконуються для дескремблювання даних, що приймаються цифровим телевізором від DVD-плеєра;
- фіг.11 - операції, які виконуються при організації захищеного каналу зв'язку між DVD-плеєром і цифровим записувальним пристроєм, і подальші операції, які виконуються для дескремблювання даних, що приймаються цифровим записувальним пристроєм від DVD-плеєра.

Спочатку будуть описані, з посиланнями на фіг.1, елементи цифрової аудіовізуальної системи 10 для записування і відтворення цифрових даних. Хоч цей винахід буде розглядатися для випадку відтворення аудіовізуальних даних за допомогою DVD-плеєра, він може бути ефективно застосований, наприклад, для випадку відтворення виключно звукової інформації, яка записується потім на пристрої для записування цифрових аудіокасет(DAT) або мінідисків(minidisc), або навіть для випадку передавання програмного забезпечення, яке записується на жорсткий диск комп'ютера.

Типова аудіовізуальна система включає в себе DVD-плеєр 12 для відтворення цифрових аудіовізуальних даних, записаних, наприклад, на диску або стрічці. DVD-плеєр підключений до цифрового пристрою 14 відображення даних, які відтворюються DVD-плеєром 12. Пристрій 14 відображення переважно представлений цифровим телевізором. Канал зв'язку 16 між плеєром 12 і пристроєм 14 відображення може приймати безліч форм, наприклад, бути радіоканалом, телефонним каналом або каналом інфрачервоного випромінювання. Однак переважно цей канал зв'язку реалізується шляхом підключення плеєра і телевізора до шини, наприклад, до шини стандарту IEEE 1394.

Система також включає в себе цифровий записувальний пристрій 18, такий як пристрій для записування DVHS або пристрій для записування DVD, виконаний з можливістю обміну даними з DVD-плеєром 12, наприклад, за допомогою шини 20 стандарту IEEE 1394. У записувальний пристрій 18 встановлюється носій запису(не показаний), на який записується інформація. Записувальний пристрій 18 має безпосереднє з'єднання 22 із пристроєм 14 відображення. Однак перед їх відображенням цифрові аудіовізуальні дані можуть передаватися із плеєра 12 в записувальний пристрій 18.

Хоч такі компоненти, як плеєр 12, пристрій 14 відображення і записувальний пристрій 18 показані як окремі елементи, деякі або всі ці компоненти цілком можуть бути об'єднані, наприклад, з утворенням

суміщеного плейєра-телевізора.

Для забезпечення захищеного передавання даних між пристроями в цифровій аудіовізуальній системі, щоб, наприклад, запобігти несанкціонованому копіюванню і поширенню записаних в цифровій формі даних, для перевірки повноважності одного або декількох пристроїв цієї аудіовізуальної системи перед передаванням яких-небудь даних між пристроями використовується система перевірки повноважності.

У переважному варіанті здійснення система перевірки повноважності пристроїв базована на передаванні сертифікатів між пристроєм і захисним модулем. Як показано на фіг.2, кожному пристрою і захисному модулю для цілей перевірки повноважності присвоюється унікальний сертифікат.

На першому рівні системи розподілу сертифікатів організація 50, яка відповідає за розподіл сертифікатів (CA - certification authority), направляє зашифровані сертифікати як виготівникам 52 побутової електронної апаратури (CE - consumer electronics), так і постачальникам 54 послуг по забезпеченню безпеки (SP - security providers).

CA 50 передає кожному виготівнику 52 електронної апаратури відповідний зашифрований сертифікат $Cert_{CA}(CEman_Kpub)$, позначений позицією 56. Цей сертифікат включає в себе, серед іншого, відкритий ключ виготівника $CEman_Kpub$; сертифікат зашифрований з використанням секретного ключа системи, або секретного ключа організації CA, CA_Kpri . Щоб надати виготівнику 52 електронної апаратури можливість дешифрувати вміст цього сертифіката, організація CA 50 передає виготівнику 52 електронної апаратури відкритий ключ організації CA, CA_Kpub . Потрібно зазначити, що згаданий секретний ключ CA_Kpri є унікальним ключем організації CA 50 і зберігається тільки у неї.

Аналогічним чином організація CA 50 передає кожному постачальнику 54 послуг по забезпеченню безпеки відповідний зашифрований сертифікат $Cert_{CA}(SP_Kpub)$, позначений позицією 58. Цей сертифікат включає в себе, серед іншого, відкритий ключ постачальника послуг по забезпеченню безпеки, SP_Kpub ; сертифікат є зашифрований з використанням секретного ключа організації CA, CA_Kpri . Щоб надати постачальнику 54 послуг по забезпеченню безпеки можливість дешифрувати вміст цього сертифіката, організація CA 50 передає постачальнику 54 послуг по забезпеченню безпеки відкритий ключ організації CA, CA_Kpub .

На другому рівні системи розподілу сертифікатів кожний виготівник 52 електронної апаратури і постачальник 54 послуг по забезпеченню безпеки (SP) присвоює відповідні сертифікати власній продукції.

Кожний виготівник 52 електронної апаратури присвоює кожному із своїх електронних пристроїв 60 відповідний зашифрований сертифікат $Cert_{CEman}(Device_Kpub)$, позначений позицією 62. Цей сертифікат включає в себе, серед іншого, унікальний відкритий ключ пристрою, $Device_Kpub$, разом з вказівником на функціональні можливості даного пристрою (записувальний пристрій, відтворювальний пристрій, або плейєр, тощо). Цей сертифікат зашифрований з використанням ключа, еквівалентного відкритому ключу $CEman_Kpub$. Для забезпечення можливості дешифрування вмісту сертифіката, виробник 52 електронної апаратури зберігає в електронному пристрої відкритий ключ організації CA, CA_Kpub , і зашифрований сертифікат $Cert_{CA}(CEman_Kpub)$ виготівника 52 електронної апаратури. Таким чином, відкритий ключ $Device_Kpub$ електронного пристрою 60 може служити як ідентифікатор даного пристрою.

Аналогічним чином, кожний постачальник 54 послуг по забезпеченню безпеки присвоює кожному захисному модулю 64 відповідний зашифрований сертифікат $Cert_{SP}(SM_Kpub)$, позначений позицією 66. Такі захисні модулі 66 можуть приймати будь-яку зручну форму, в залежності від необхідних фізичних розмірів і характеристик. Наприклад, захисний модуль може бути виконаний знімним, із можливістю установа в гніздо, передбачене в електронному пристрої 60, або може бути окремим модулем, який підключається до пристрою 60. У певних випадках може використовуватися смарт-карта, подібна банківській картці, але однаково можливі і інші формати, такі як карти типу PCMCIA.

Зашифрований сертифікат, який присвоюється захисному модулю 64, включає в себе, крім іншого, унікальний відкритий ключ захисного модуля, SM_Kpub . Сертифікат зашифрований з використанням ключа, еквівалентного відкритому ключу SP_Kpub . Щоб забезпечити можливість дешифрування вмісту сертифіката постачальник 54 послуг по забезпеченню безпеки зберігає в захисному модулі 64 відкритий ключ організації CA, CA_Kpub , і зашифрований сертифікат $Cert_{CA}(SP_Kpub)$ постачальника послуг по забезпеченню безпеки. Відповідно, відкритий ключ SM_Kpub захисного модуля 64 може служити як ідентифікатор даного захисного модуля.

Для забезпечення можливості перевірки вмісту сертифіката після дешифрування сертифіката в будь-який з вищезазначених сертифікатів може бути включений підпис. Вміст сертифіката може забезпечуватися підписом за допомогою ключа, використаного для шифрування сертифіката.

Перевірка повноважності пристрою в даній цифровій аудіовізуальній системі здійснюється шляхом обміну сертифікатами між цим пристроєм і захисним модулем. Як показано на фіг.3, в першому варіанті здійснення цього винаходу захисний модуль 64 з'єднаний із пристроєм 60 за допомогою каналу зв'язку 70, що забезпечує захисному модулю можливість перевіряти повноважність тільки цього пристрою. Однак, як показано на фіг.4, в альтернативному варіанті захисний модуль може бути з'єднаний з двома або більше пристроями, 60a, 60b, за допомогою відповідних каналів зв'язку 70a, 70b.

Перевірка повноважності одиночного пристрою захисним модулем буде описана нижче з посиланнями на фіг.5.

Процедура перевірки повноважності може ініціюватися в будь-який час, наприклад, після ввімкнення пристрою, установа диска, перемикання даного пристрою користувачем на інший канал, встановлення з'єднання із захисним модулем тощо.

Процедура перевірки повноважності ініціюється захисним модулем. На кроці 100 захисний модуль 64 передає в пристрій 60 зашифрований сертифікат $Cert_{CA}(SP_Kpub)$ постачальника 54 послуг по

забезпеченню безпеки. На кроці 102 зазначений пристрій дешифрує вміст зашифрованого сертифіката $Cert_{CA}(SP_Kpub)$, використовуючи відкритий ключ організації CA 50, CA_Kpub , роблячи можливим витягання із зазначеного сертифіката відкритого ключа SP_Kpub постачальника 54 послуг по забезпеченню безпеки.

Після передавання зашифрованого сертифіката $Cert_{CA}(SP_Kpub)$ в пристрій 60, на кроці 104 захисний модуль 64 передає в пристрій 60 свій власний унікальний зашифрований сертифікат $Cert_{SP}(SM_Kpub)$. На кроці 106 зазначений пристрій дешифрує вміст зашифрованого сертифіката $Cert_{SP}(SM_Kpub)$, використовуючи відкритий ключ SP_Kpub постачальника послуг по забезпеченню безпеки, раніше витягнутий пристроєм 60 із зашифрованого сертифіката $Cert_{CA}(SP_Kpub)$, роблячи можливим витягання з названого сертифіката відкритого ключа SM_Kpub захисного модуля 64.

На кроці 108 пристрій 60 передає в захисний модуль 64 зашифрований сертифікат $Cert_{CA}(CEman_Kpub)$ виготівника 52 електронної апаратури. На кроці 110 захисний модуль 64 дешифрує зашифрований сертифікат $Cert_{CA}(CEman_Kpub)$, використовуючи відкритий ключ організації CA 50, CA_Kpub , роблячи можливим витягання з названого сертифіката відкритого ключа $CEman_Kpub$ виготівника 52 електронної апаратури.

Після передавання зашифрованого сертифіката $Cert_{CA}(CEman_Kpub)$ в захисний модуль 64, на кроці 112 пристрій 60 генерує випадкове число X . Це випадкове число X не грає ніякої ролі в перевірці повноважності пристрою захисним модулем - воно використовується для створення захищеного автентифікованого каналу (SAC - Secure Authenticated Channel) між пристроєм 60 і захисним модулем 64. Це описується більш детально нижче.

На кроці 114 пристрій 60 перетасовує розряди випадкового числа X і зашифрованого сертифіката $Cert_{CEman}(Device_Kpub)$, який зберігається в пристрої 60, щоб скремблювати ці випадкове число X і зашифрований сертифікат $Cert_{CEman}(Device_Kpub)$. Піддані порозрядному перетасуванню випадкове число X і зашифрований сертифікат $Cert_{CEman}(Device_Kpub)$ потім зашифровуються на кроці 116 із використанням відкритого ключа SM_Kpub захисного модуля 64, раніше переданого в пристрій 60 захисним модулем на кроці 104, і на кроці 118 піддані порозрядному перетасуванню зашифроване випадкове число і зашифрований сертифікат $Cert_{CEman}(Device_Kpub)$ передаються в захисний модуль 64.

На кроці 120 захисний модуль 64 дешифрує зашифровані піддані порозрядному перетасуванню випадкове число і зашифрований сертифікат $Cert_{CEman}(Device_Kpub)$, використовуючи еквівалентний відкритому ключу SM_Kpub ключ SM_Kpriv . На кроці 122 порозрядне перетасування випадкового числа і сертифіката $Cert_{CEman}(Device_Kpub)$ обертається.

Алгоритм, який використовується для перетасування розрядів випадкового числа X і зашифрованого сертифіката $Cert_{CEman}(Device_Kpub)$, може бути збережений в захисному модулі 64, щоб забезпечити можливість обертання цього порозрядного перетасування. У альтернативному варіанті захисний модуль 64 може, після приймання зашифрованого сертифіката $Cert_{CA}(CEman_Kpub)$, передавати в пристрій 60 випадкове число, яке іменується випадковою перевіркою, Z . Випадкова перевірка Z піддається порозрядному перетасуванню пристроєм 60, зашифровується з використанням відкритого ключа SM_Kpub захисного модуля і передається в захисний модуль, переважно одночасно з підданими порозрядному перетасуванню випадковим числом X і зашифрованим сертифікатом $Cert_{CEman}(Device_Kpub)$. Захисний модуль 64 дешифрує зашифровану піддану порозрядному перетасуванню випадкову перевірку Z і порівнює цю піддану порозрядному перетасуванню випадкову перевірку з випадковою перевіркою, яка зберігається в ньому і не зазнавала порозрядного перетасування, щоб визначити, як випадкова перевірка Z була піддана порозрядному перетасуванню пристроєм 60. Захисний модуль 64 використовує результат цієї перевірки для обертання порозрядного перетасування, застосованого зазначеним пристроєм до випадкового числа X і зашифрованого сертифіката $Cert_{CEman}(Device_Kpub)$.

Повернемося до фіг.5; на кроці 124 випадкове число X витягується і зберігається захисним модулем 64. На кроці 126 захисний модуль 64 дешифрує зашифрований сертифікат $Cert_{CEman}(Device_Kpub)$, використовуючи відкритий ключ $CEman_Kpub$ виготівника 52 електронної апаратури, раніше переданий в захисний модуль 64 пристроєм 60, роблячи можливим витягання з цього сертифіката відкритого ключа $Device_Kpub$ пристрою 60.

Перевірка повноважності пристрою 60 здійснюється захисним модулем 64 з використанням відкритого ключа $Device_Kpub$ пристрою 60 на кроці 128. Захисний модуль зіставляє прийнятий відкритий ключ $Device_Kpub$ пристрою з раніше збереженим в захисному модулі списком відкритих ключів пристроїв. Цей список відкритих ключів пристроїв може бути сформований організацією CA 50 і збережений, наприклад, в пам'яті захисного модуля 64 постачальника 54 послуг по забезпеченню безпеки, такий як енергонезалежна пам'ять.

Захисний модуль 64 підтримує списки двох типів. "Відмовний список" включає в себе відкриті ключі пристроїв, асоційовані з неповноважними пристроями, і використовується для формування "чорного списку" пристроїв, які не відповідають умовам надання прав доступу. "Санкціонуючий список" включає в себе відкриті ключі пристроїв, асоційовані з повноважними пристроями, і використовується для обмеження передавання даних таким чином, що передавання даних можливе лише між заздалегідь зареєстрованими пристроями.

Ідентифікатори пристроїв, навмисно опубліковані третіми особами, наприклад, в Internet, можуть бути додані в "відмовний список" організацією CA 50 при періодичному оновленні захисного модуля 64, для того щоб запобігти передаванню даних в ці пристрої або клони цих пристроїв, або з них. У той же час шляхом використання санкціонуючого списку також можна запобігти застосуванню ідентифікаторів пристроїв, навмисно опублікованих в Internet, оскільки ці ідентифікатори не будуть дійсні ніде, крім, наприклад,

домашньої мережі.

Список, з яким зіставляється прийнятий відкритий ключ пристрою, визначається прапором, включеним в зашифрований сертифікат пристрою або зашифрований сертифікат захисного модуля. Наприклад, захисний модуль може порівнювати прийнятий відкритий ключ пристрою із збереженими відкритими ключами, асоційованими з неповноважними пристроями, коли прапор встановлений в "0", і порівнювати прийнятий відкритий ключ пристрою як із збереженими відкритими ключами, асоційованими з неповноважними пристроями, так і із збереженими відкритими ключами, асоційованими з повноважними пристроями, коли прапор встановлений в "1".

Якщо з'ясується, що пристрій 60 є неповноважним, то захисний модуль 64 перериває обмін даними із пристроєм 60. Якщо, як показано на фіг.4, захисний модуль бере участь в обміні даними з іншими пристроями, зв'язок з цими пристроями також уривається.

Якщо з'ясується, що пристрій 60 є повноважним, то захисний модуль 64 організує захищений автентифікований канал(SAC) зв'язку між пристроєм 60 і захисним модулем 64. На фіг.6 показані операції, які виконуються при організації захищеного автентифікованого каналу зв'язку між пристроєм і захисним модулем.

На кроці 200 захисний модуль 64 генерує випадковий сеансовий ключ SK. На кроці 202 випадковий сеансовий ключ SK зашифровується захисним модулем за допомогою алгоритму TDES із використанням випадкового числа X, переданого в захисний модуль 64 пристроєм 60. На кроці 204 зашифрований сеансовий ключ TDES_x(SK) передається в пристрій 60.

На кроці 206 пристрій 60 дешифрує зашифрований сеансовий ключ TDES_x(SK), використовуючи зазначене випадкове число X, і на кроці 208 -зберігає сеансовий ключ SK в пам'яті. Після цього сеансовий ключ SK використовується для дешифрування даних, які передаються між пристроєм 60 і захисним модулем 64.

Таким чином, після перевірки повноважності пристрою, захисним модулем здійснюється розподіл ключів для організації захищеного каналу зв'язку між пристроєм і захисним модулем. Оновлення сеансового ключа(SK) може бути також ініційоване в будь-який час, наприклад, після ввімкнення пристрою, установлення диска, перемикання даного пристрою користувачем на інший канал, встановлення з'єднання із захисним модулем тощо.

Повернемося до фіг.1; звичайно DVD-плеєр 12 передає в пристрій 14 відображення і записувальний пристрій 18 скрембльовані дані. Операції, які виконуються при дескремблюванні даних, що приймаються яким-небудь пристроєм, будуть описані нижче з посиланнями на фіг.7.

На DVD-диску звичайно разом із скрембльованими аудіо- і/або відеоданими зберігаються зашифровані повідомлення керування правами(ECM). ECM - це повідомлення, «прив'язане» до скрембльованих аудіо- і/або відеоданих(контенту). Це повідомлення включає в себе керуюче слово(яке дозволяє дескремблювати зазначені дані) і критерії доступу до відповідних даних. Критерії доступу і керуюче слово передаються DVD-плеєром 12 в, наприклад, пристрій 14 відображення по каналу зв'язку 16.

Дані, збережені на диску, звичайно містять кілька окремих компонент; наприклад, телевізійна програма включає в себе компоненту зображення, звукову компоненту, компоненту субтитрів тощо. Кожна з цих компонент скремблюється і зашифровується окремо. Для кожної скрембльованої компоненти потрібне окреме ECM. У альтернативному варіанті для всіх скрембльованих компонент сервісу може використовуватися одне ECM.

Керуюче слово звичайно змінюється кожні декілька секунд, так що повідомлення ECM також періодично вставляються в дані, щоб зробити можливим дескремблювання керуючого слова, що змінюється. З метою резервування кожне повідомлення ECM звичайно включає в себе два керуючих слова - поточне керуюче слово і наступне керуюче слово.

Після приймання скрембльованих даних і зашифрованого повідомлення ECM від DVD-плеєра 12 пристрій 14 відображення витягує повідомлення ECM зі скрембльованих даних і передає витягнуте повідомлення ECM в дескремблювальні схеми для дешифрування повідомлення ECM і витягання керуючого слова з дешифрованого повідомлення ECM.

Зазначені дескремблювальні схеми можуть бути реалізовані в знімному модулі 40 умовного доступу(CAM), звичайно виконаному в формі PCMCIA-карти, або PC-карти, яка встановлюється в гніздо пристрою-приймача. У альтернативному варіанті модуль CAM 40 може бути виконаний фізично окремим від пристрою-приймача, при цьому модуль CAM 40 і пристрій 14 відображення зв'язані з можливістю передавання даних за допомогою будь-якого відповідного каналу зв'язку 42, наприклад, через послідовний або паралельний інтерфейс.

Крім того, сам модуль CAM 40 може мати картоприймач для установлення смарт-карти. У таких системах смарт-карта контролює, чи має кінцевий користувач права дешифрувати повідомлення ECM і отримувати доступ до програми. Якщо кінцевий користувач має відповідні права, повідомлення ECM дешифрується процесором 41 смарт-карти, і з нього витягується керуюче слово. Процесор 41 модуля CAM 40 потім може дескремблювати скрембльовані дані, щоб подавати в пристрій-приймач потік незашифрованих даних, наприклад, для декомпресування і подальшого відображення. У альтернативному варіанті, дескремблювання даних може здійснюватися в пристрої 14 відображення з використанням інформації керуючих слів, переданої в пристрій 14 відображення з модуля CAM 40.

У тому випадку, коли скрембльовані дані передаються з DVD-плеєра 12 в цифровий записувальний пристрій 18 для подальшого перегляду, виготовник DVD-диска може побажати обмежити доступ до записаних даних. Наприклад, виготовник диска може побажати заборонити будь-яке подальше копіювання записаних даних. У таких випадках права доступу, або розширена керуюча інформація(XCML - extended

Control Management Information), розміщуються в розширеному повідомленні керування правами (ХЕСМ - extended ECM), яке включає в себе різноманітні права доступу, визначені виготівником диска. Після приймання ХЕСМ процесор 41 модуля САМ 40 дешифрує повідомлення ХЕСМ, модифікує повідомлення ХЕСМ, наприклад, щоб заборонити будь-яке копіювання записаних даних, знову зашифровує повідомлення ХЕСМ і передає модифіковане знов зашифроване повідомлення ХЕСМ назад в записувальний пристрій.

У системі такого типу між модулем САМ і пристроєм 14 відображення, або записувальним пристроєм 18, можуть передаватися уразливі дані (керуючі слова, модифіковані повідомлення ХЕСМ або дескрембльовані дані), і на цьому інтерфейсі можуть виникати проблеми, пов'язані з безпекою. Щоб подолати такі проблеми, перед передаванням яких-небудь даних, наприклад, повідомлень ECM із пристроєм 14 відображення в смарт-карту, між пристроєм 14 відображення і модулем САМ 40 організується захищений автентифікований канал (SAC) 42, як було описано вище з посиланнями на фіг.5 і фіг.6. Для організації каналу SAC 42 між пристроєм 14 відображення і модулем САМ 40, модуль САМ 40 повинен мати збереженим, наприклад, в смарт-карті, список відкритих ключів пристроїв, щоб перевіряти повноважність пристрою 14 відображення.

Як показано на фіг.4, захисний модуль може бути з'єднаний із двома або більш підключеними пристроями 60a, 60b через відповідні канали зв'язку 70a, 70b. Крім перевірки повноважності обох цих пристроїв, яка здійснюється відносно кожного із пристроїв так, як описано з посиланнями на фіг.5, захисний модуль може також організовувати захищений канал передавання даних між пристроями. На фіг.8 показані операції, які виконуються при організації захищеного передавання даних між двома пристроями.

Організація безпечного передавання даних між пристроєм А 60a і пристроєм В 60b здійснюється після перевірки захисним модулем повноважності обох пристроїв 60a, 60b. Як показано на фіг.8, на кроці 300 захисний модуль генерує випадковий сеансовий ключ SK. На кроці 302 цей випадковий сеансовий ключ SK зашифровується захисним модулем 64 з використанням випадкового числа X, переданого в захисний модуль пристроєм А 60a під час перевірки повноважності цього пристрою. У переважному варіанті здійснення шифрування здійснюється з використанням симетричного алгоритму, такого як потрійний DES (Triple DES, TDES).

На кроці 304 зашифрований сеансовий ключ $TDES_X(SK)$ передається в пристрій А 60a. На кроці 306 пристрій А 60a дешифрує зашифрований сеансовий ключ $TDES_X(SK)$, використовуючи зазначене випадкове число X, і зберігає цей сеансовий ключ SK в пам'яті.

На кроці 308 зазначений випадковий сеансовий ключ SK додатково зашифровується захисним модулем 64 за допомогою алгоритму TDES з використанням випадкового числа Y, переданого в захисний модуль 64 пристроєм В 60b під час перевірки повноважності цього пристрою. На кроці 310 зашифрований сеансовий ключ $TDES_Y(SK)$ передається в пристрій В 60b. На кроці 312 пристрій В 60b дешифрує зашифрований сеансовий ключ $TDES_Y(SK)$, використовуючи зазначене випадкове число Y, і зберігає сеансовий ключ SK в пам'яті.

Таким чином, сеансовий ключ SK передається в кожний пристрій по відповідному каналу SAC. Потім сеансовий ключ SK може бути використаний, наприклад, пристроєм А 60a, щоб зашифрувати дані, які передаються в пристрій В 60b по каналу зв'язку 75.

Як показано на фіг.9, на кроці 400 пристрій 60a зашифровує дані D, використовуючи сеансовий ключ SK. При цьому як алгоритм шифрування використовується симетричний алгоритм, такий як алгоритм потрійний DES (TDES), або подібний.

На кроці 402 зашифровані дані $TDES_{SK}(D)$ передаються в пристрій 60b по каналу зв'язку 75. На кроці 404 пристрій 60b дешифрує дані $TDES_{SK}(D)$, використовуючи сеансовий ключ SK, і отримує дані D.

Як вказувалося вище, жоден із пристроїв не формує сеансових ключів; сеансові ключі формуються тільки захисним модулем. Відповідно, описаний спосіб забезпечує дуже простий, але, незважаючи на це, надійний спосіб забезпечення захищеного зв'язку між пристроями, оскільки дані, які передаються першим пристроєм, можуть бути дешифровані тільки пристроєм, який встановив захищений автентифікований канал з тим же захисним модулем, що і зазначений перший пристрій.

Як зазначалося з посиланнями на фіг.7, додатково до виконання перевірки повноважності пристроїв і організації каналів SAC, захисний модуль може передавати в пристрій керуючі слова, права доступу і/або скрембльовані дані. На фіг.10 і фіг.11 представлені приклади, в яких захисний пристрій організує захищений канал зв'язку між двома пристроями і потім передає в який-небудь пристрій дані, асоційовані зі скрембльованими даними.

У першому прикладі, на фіг.10, показані операції, які виконуються при організації захищеного каналу зв'язку між DVD-плеєром і цифровим телевізором, а також подальші операції, які виконуються для дескремблювання даних, що приймаються від DVD-плеєра цифровим телевізором.

На кроці 500 захисний модуль 64 перевіряє повноважність DVD-плеєра 12 і цифрового телевізора 14 за допомогою операцій, описаних вище з посиланнями на фіг.5. Якщо обидва ці пристрої признаються повноважними, захисний модуль 64 організує захищені автентифіковані канали (SAC) з DVD-плеєром 12 і цифровим телевізором за допомогою операцій, описаних вище з посиланнями на фіг.6. Внаслідок встановлення каналу SAC в кожному із зазначених пристроїв і в захисному модулі зберігається сеансовий ключ SK.

На кроці 502 дані, які включають в себе скрембльовані системою керування (CSS - Control System Scrambled) дані (контент) і зашифровані (оригінальним способом) власником даних повідомлення ECM, які включають в себе керуючі слова для дескремблювання зазначених даних, зашифровуються DVD-плеєром 12 з використанням сеансового ключа SK і передаються в цифровий телевізор по каналу зв'язку

16.

Зашифровані дані приймаються цифровим телевізором 14 на кроці 504 і дешифруються з використанням сеансового ключа SK. Скрембльовані дані передаються в демультимплексор 90, який, на кроці 506, відділяє CSS-дані від зашифрованих повідомлень ECM. На кроці 508 зашифровані повідомлення ECM передаються цифровим телевізором 14 по каналу SAC в захисний модуль 64. Для передавання в захисний модуль 64 по каналу SAC зашифровані повідомлення ECM додатково шифруються цифровим телевізором 14 з використанням сеансового ключа SK, сформованого захисним модулем 64.

Як показано на фіг.10, захисний модуль є умовно розділений на стандартний захисний блок 66 і захисний блок 68 власника даних(оригінальний захисний блок). На кроці 510 двічі зашифровані повідомлення ECM приймаються стандартним захисним блоком 66 і дешифруються з використанням сеансового ключа SK(одне дешифрування). На кроці 512 зашифровані(оригінальним способом) власником даних повідомлення ECM передаються в захисний блок 68 власника даних, який, на кроці 514, дешифрує і перевіряє ці зашифровані повідомлення ECM, використовуючи ключ, еквівалентний ключу власника даних, який використовувався для шифрування цього повідомлення ECM, і, при наявності відповідних прав, опрацює це повідомлення ECM, щоб витягнути з нього керуючі слова, або CSS-ключі.

На кроці 516 CSS-ключі передаються в стандартний захисний блок 66, який зашифровує CSS-ключі, використовуючи сеансовий ключ SK, і передає зашифровані CSS-ключі в цифровий телевізор 14 по каналу SAC. На кроці 518 прийняті зашифровані CSS-ключі дешифруються цифровим телевізором 14 з використанням сеансового ключа і потім передаються в дескремблер 92 для використання при дескремблюванні CSS-даних. На кроці 520 дескрембльовані дані передаються в блок 94 відображення для відображення.

Як витікає з вищесказаного, керуючі слова завжди шифруються з використанням сеансового ключа SK перед передаванням між будь-яким із пристроїв і захисним модулем.

У наведеному вище прикладі керуючі слова містяться в повідомленнях ECM. Однак повідомлення ECM можуть міститися в повідомленнях XECM, разом з інформацією XCMI, або правами доступу, які опрацюються захисним блоком 68 власника даних(оригінальним захисним блоком), наприклад, щоб визначити, чи не закінчився термін дії прав користувача на перегляд даних.

У другому прикладі, на фіг.11, показані операції, які виконуються при організації захищеного каналу зв'язку між DVD-плеєром і цифровим записувальним пристроєм, і подальші операції, які виконуються для дескремблювання даних, що приймаються цифровим записувальним пристроєм від DVD-плеєра.

На кроці 600 захисний модуль 64 перевіряє повноважність DVD-плеєра 12 і цифрового записувального пристрою 18 за допомогою операцій, описаних вище з посиланнями на фіг.5. Якщо обидва ці пристрої визнаються повноважними, захисний модуль 64 організує захищені автентифіковані канали(SAC) зв'язку із DVD-плеєром 12 і цифровим записувальним пристроєм 18, за допомогою операцій, описаних вище з посиланнями на фіг.6. Внаслідок організації цих каналів SAC в кожному із зазначених пристроїв і в захисному модулі зберігається сеансовий ключ SK.

На кроці 602 дані, які включають в себе скрембльовані системою керування(CSS) дані(контент) і зашифровані(оригінальним способом) власником даних повідомлення XECM, які включають в себе керуючі слова для дескремблювання зазначених даних і XCMI, зашифровуються DVD-плеєром 12 із використанням сеансового ключа SK і передаються в записувальний пристрій по каналу зв'язку 20.

На кроці 604 зашифровані дані приймаються записувальним пристроєм 18 і дешифруються з використанням сеансового ключа SK. Скрембльовані дані передаються в демультимплексор 90, який, на кроці 606, відділяє CSS-дані від зашифрованих повідомлень XECM. На кроці 608 зашифровані повідомлення XECM передаються записувальним пристроєм 18 по каналу SAC в захисний модуль 64. Для передавання в захисний модуль 64 по каналу SAC зашифровані повідомлення XECM додатково зашифровуються записувальним пристроєм 18 із використанням сеансового ключа SK, згенерованого захисним модулем 64.

Як показано на фіг.11, захисний модуль є умовно розділений на стандартний захисний блок 66 і захисний блок 68 власника даних(оригінальний захисний блок). На кроці 610 двічі зашифровані повідомлення XECM приймаються стандартним захисним блоком 66 і дешифруються з використанням сеансового ключа SK(одне дешифрування). На кроці 612 зашифровані(оригінальним способом) власником даних повідомлення XECM передаються в захисний блок 68 власника даних(оригінальний захисний блок), який, на кроці 614, дешифрує і перевіряє ці зашифровані повідомлення XECM, використовуючи ключ, еквівалентний ключу власника даних, який використовувався для шифрування цього повідомлення XECM, і, при наявності відповідних прав, опрацює це повідомлення XECM, щоб оновити інформацію XCMI, наприклад, із метою обмеження кількості відтворень користувачем зазначених даних, або заборони будь-якого подальшого перезаписування цих даних, тощо.

На кроці 616 ці модифіковані повідомлення XECM зашифровуються з використанням алгоритму власника даних(оригінального алгоритму) PA(Proprietary Algorithm) і призначеного для користувача ключа 96, збереженого в захисному модулі 68. Завдяки цьому забезпечується додатковий захист даних, які записуються записувальним пристроєм 18: керуючі слова для дескремблювання CSS-даних можуть бути витягнуті з модифікованого повідомлення XECM тільки в тому випадку, якщо користувач має доступ до зазначеного призначеного для користувача ключа. Таким чином, відтворення і перегляд записаних даних може проводити лише власник захисного модуля.

На кроці 618 зашифровані повідомлення XECM передаються в стандартний захисний блок 66, який додатково зашифровує зазначені зашифровані XECM, використовуючи сеансовий ключ SK, і передає зашифровані XECM в записувальний пристрій по каналу SAC. На кроці 620 прийняті зашифровані

повідомлення ХЕСМ дешифруються записувальним пристроєм із використанням сеансового ключа (одне дешифрування) і потім передаються на носій запису 98, такий як цифрова аудіокасета DAT, для збереження зазначених CSS-даних і зашифрованих повідомлень ХЕСМ.

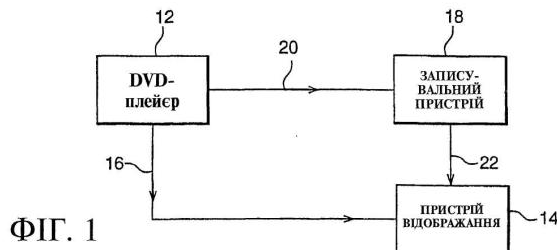
Потрібно розуміти, що цей винахід був описаний вище за допомогою виключно ілюстративних прикладів, і зміни в деталях реалізації можливі без виходу за межі цього винаходу.

Наприклад, хоч в приведених вище прикладах зазначалася організація каналу зв'язку між пристроями з використанням цифрового інтерфейсу IEEE 1394, можуть бути також використані однонаправлені канали передавання, такі як шини 8-VSB і 16-VSB.

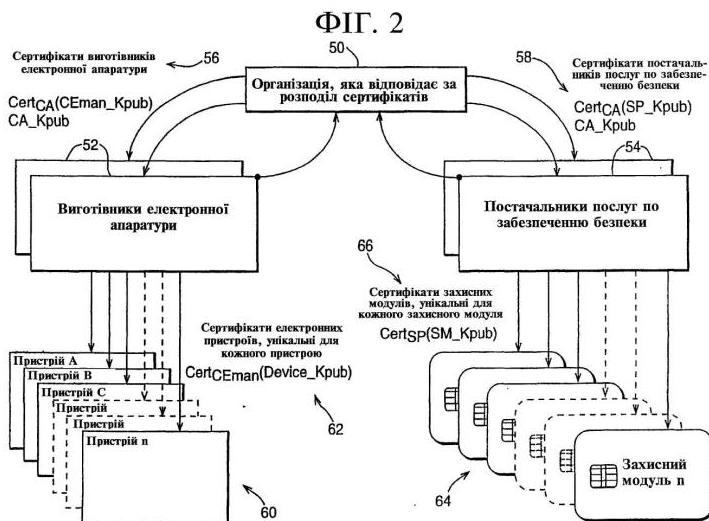
Безпосереднє передавання пристроєм сертифікатів в захисний модуль не є принциповою деталлю реалізації. Наприклад, якщо перший пристрій не може приймати дані із захисного модуля, цей перший пристрій може передавати свої сертифікати у другий пристрій, який може здійснювати двосторонній зв'язок із захисним модулем для перевірки повноважності першого пристрою.

У описаних прикладах передбачається тільки один захисний модуль. Однак в мережі, яка складається з кількох пристроїв, підключених за допомогою різних інтерфейсів, можуть співіснувати різні захисні модулі.

Кожна ознака, розкрита введеному вище описі, а також (у відповідних випадках) в формулі винаходу і на кресленнях, може надаватися окремо або в будь-якому відповідному поєднанні з іншими ознаками.



ФІГ. 1



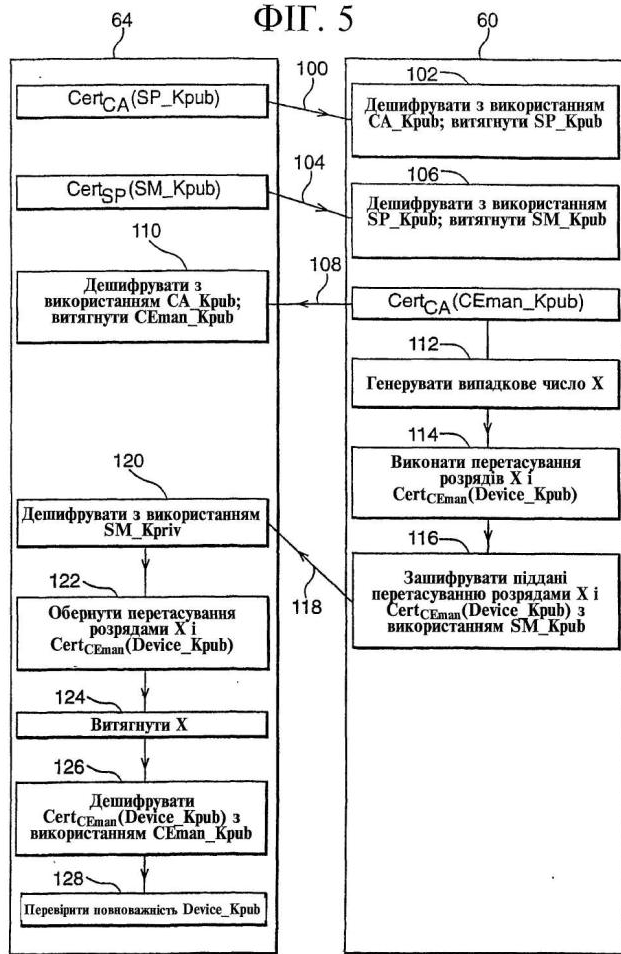
ФІГ. 2



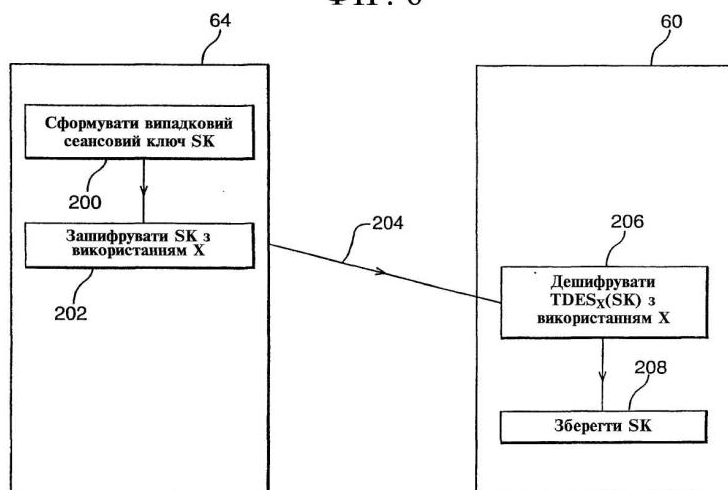
ФІГ. 3

ФІГ. 4

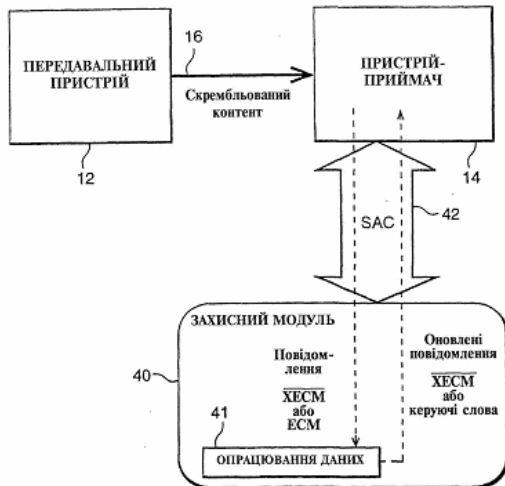
ФІГ. 5



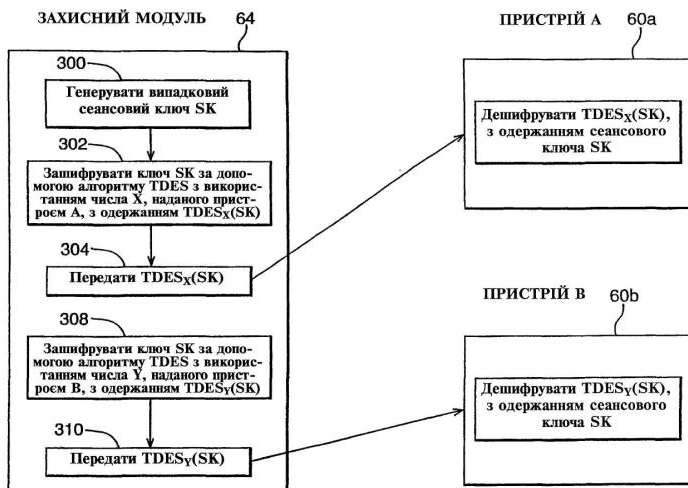
ФІГ. 6



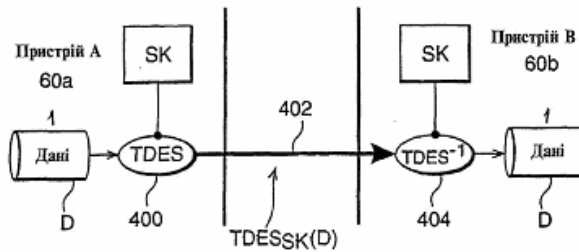
ФІГ. 7

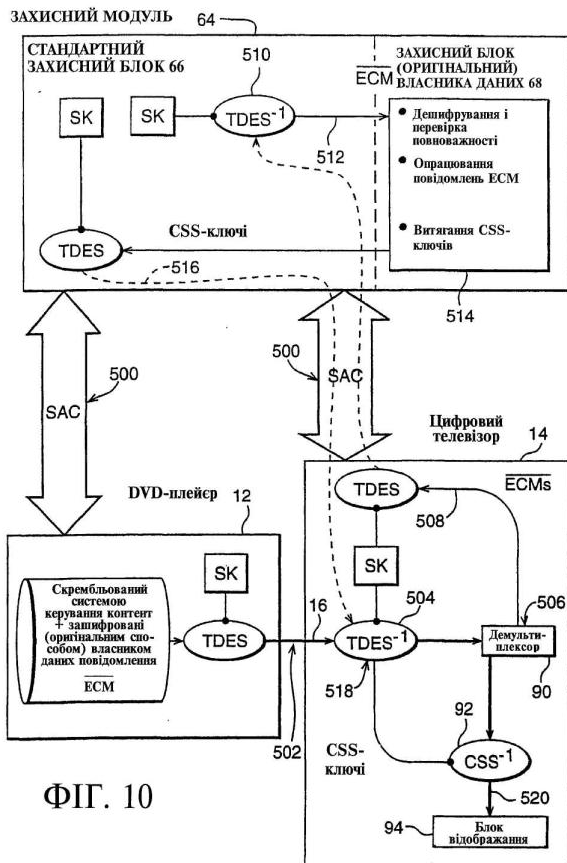


ФІГ. 8

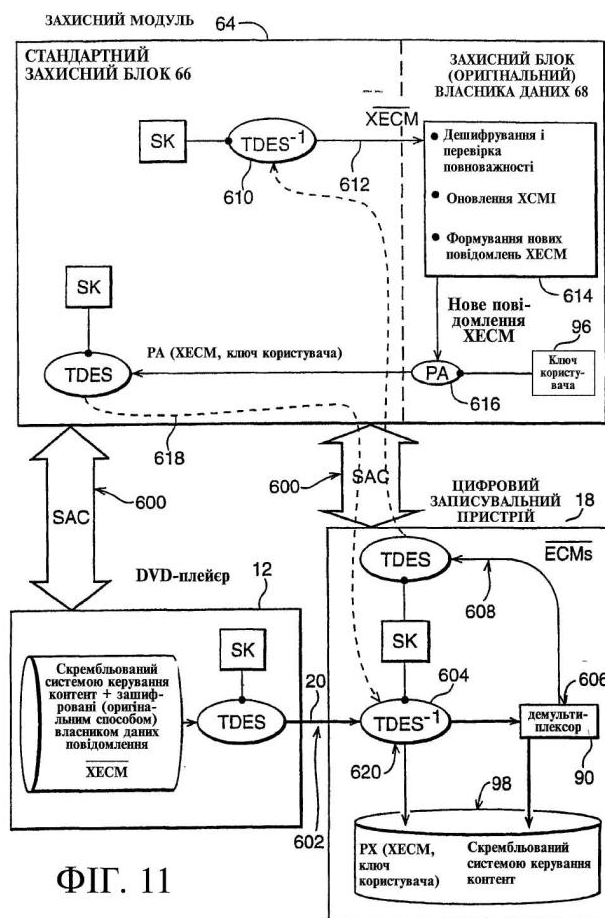


ФІГ. 9





ФІГ. 10



ФІГ. 11

