

**УКРАЇНА****(19) UA****(11) 100829****(13) C2****(51) МПК****H04L 29/06** (2006.01)**H04W 12/04** (2009.01)

**ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ**

**(12) ОПИС ДО ПАТЕНТУ НА ВІНАХІД**

<b>(21)</b> Номер заявки:	<b>а 2012 00873</b>	<b>(72)</b> Винахідник(и):	<b>Кубота Кейчі (GB)</b>
<b>(22)</b> Дата подання заявки:	<b>16.06.2010</b>	<b>(73)</b> Власник(и):	<b>НОКІА КОРПОРЕЙШН,</b>
<b>(24)</b> Дата, з якої є чинними права на винахід:	<b>25.01.2013</b>		Keilalahdentie 4, FIN-02150 Espoo, Finland (FI)
<b>(31)</b> Номер попередньої заявки відповідно до Паризької конвенції:	<b>12/494,957</b>	<b>(74)</b> Представник:	<b>Крилова Надія Іванівна, реєстр. №30</b>
<b>(32)</b> Дата подання попередньої заявки відповідно до Паризької конвенції:	<b>30.06.2009</b>	<b>(56)</b> Перелік документів, взятих до уваги експертизою:	US 2007258591 A1; 08.11.2007 EP 1337125 A2; 20.08.2003
<b>(33)</b> Код держави-учасниці Паризької конвенції, до якої подано попередню заявку:	<b>US</b>		
<b>(41)</b> Публікація відомостей про заявку:	<b>11.06.2012, Бюл.№ 11</b>		
<b>(46)</b> Публікація відомостей про видачу патенту:	<b>25.01.2013, Бюл.№ 2</b>		
<b>(86)</b> Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ	<b>PCT/FI2010/050509, 16.06.2010</b>		

**(54) СИСТЕМИ, МЕТОДИ ТА АПАРАТУРА ДЛЯ ВІЯВЛЕННЯ ПОМИЛКИ ШИФРУВАННЯ ТА ВІДНОВЛЕННЯ БЕЗПОМИЛКОВОГО СТАНУ****(57) Реферат:**

Системи, методи і апаратура передбачені для виявлення помилки шифрування та відновлення безпомилкового стану. Метод може включати використання першого набору з одного або більше вхідних параметрів шифру для декодування зашифрованих даних, зашифрованих із використанням другого набору з одного або більше вхідних параметрів шифру. Метод може додатково включати порівняння значення принаймні частини декодованих даних із очікуваним значенням. Метод може додатково включати визначення виникнення помилки шифрування, коли значення принаймні частини декодованих даних не дорівнює очікуваному значенню. Метод може також включати ініціювання процедури повторної синхронізації шифрування у відповідь на визначення, що відбулася помилка шифрування, щоб повторно синхронізувати принаймні один з першого набору вхідних параметрів шифру із принаймні одним із другого набору вхідних параметрів шифру. Відповідні системи й апаратура також передбачені.

**UA 100829 C2**



Fig. 3

Галузь техніки, до якої належить винахід

[0001] Варіанти втілення даного винаходу в цілому мають відношення до комунікаційних технологій, та, більш детально, стосуються систем, методів та апаратури для виявлення помилки шифрування та відновлення безпомилкового стану.

5 Передумови створення винаходу

[0002] Ера сучасних комунікацій викликала величезне поширення дротових та бездротових мереж. Комп'ютерні мережі, телевізійні мережі та мережі телефонії перебувають у безпрецедентному технологічному розвитку, зокрема, завдяки високому споживчому попиту. Бездротові та мобільні мережеві технології реагують на вимоги відповідних споживачів, забезпечуючи більшу гнучкість та оперативність передання інформації й надаючи користувачам зручність. Паралельно з розширенням мереж були розроблені мобільні комп'ютерні пристрої, що використовують переваги функціональних можливостей, які пропонуються бездротовими мережами, щоб полегшити мобільне обчислювання. У результаті пристрої мобільної комунікації та бездротові мережі широко використовуються споживачами, щоб забезпечити використання

15 мобільної обробки даних для широкого спектру обміну інформацією.  
[0003] Для перешкодження несанкціонованому доступу третьої сторони до даних комунікаційних мереж, принаймні деякі з даних можуть бути зашифровані. Використання обміну шифрованою інформацією може вимагати приймаючий елемент для використання першого набору з одного або більше вхідних параметрів шифру, щоб декодувати отримані зашифровані дані. Перший набір вхідних параметрів шифру, можливо, повинен бути таким чином синхронізований із другим набором з одного або більше вхідних параметрів шифру, що використовується передаючим елементом для шифрування даних, щоб гарантувати точне декодування зашифрованих даних приймаючим елементом. Коли перший та другий набори вхідних параметрів шифру не є синхронізованими, може виникнути помилка шифрування, яка полягає в тому, що приймаючий елемент не буде в змозі точно декодувати зашифровані дані.

Коротке викладення деяких прикладів винаходу

[0004] Отже, виявлення помилки шифрування та відновлення безпомилкового стану забезпечено системами, методами, апаратурою та комп'ютерними програмними продуктами. В цьому відношенні, передбачаються методи, апаратура та комп'ютерні програмні продукти, які можуть забезпечити деякі переваги для обчислювальних пристроїв, користувачів обчислювальних пристроїв та мережевих операторів. Варіанти втілення винаходу забезпечують приймаючу апаратуру, зконфігуровану для визначення виникнення помилки шифрування. В цьому відношенні, варіанти втілення винаходу забезпечують приймаючу апаратуру, зконфігуровану для визначення виникнення помилки шифрування шляхом порівняння показників декодованих даних із очікуваними показниками, щоб визначити, чи дорівнюють декодовані дані очікуваному значенню. Це порівняння дозволяє деяким варіантам втілення винаходу визначити виникнення помилки шифрування незалежно від типу сервісу, з яким пов'язаний модуль протоколу шифрування даних. Крім того, варіанти втілення винаходу забезпечують приймаючу апаратуру, зконфігуровану для ініціювання процедури виправлення помилки шифрування так, щоб повторно синхронізувати локальний набір з одного або більше вхідних параметрів шифру, який використовується для декодування отриманих зашифрованих даних, із набором з одного або більше вхідних параметрів шифру, який використовує передаюча апаратура для кодування зашифрованих даних до передачі на термінал. Деякі варіанти втілення винаходу забезпечують приймаючу апаратуру, зконфігуровану для ініціювання керованої по радіоканалу повторної синхронізації із передаючою апаратурою, щоб повторно синхронізувати один або більше вхідних параметрів шифру. Варіанти втілення винаходу також забезпечують приймаючу апаратуру, зконфігуровану для автономної повторної синхронізації одного або більше вхідних параметрів шифру шляхом вибору найбільш ймовірного альтернативного значення принаймні для одного вхідного параметру шифру.

50 [0005] У першому прикладі втіленні винаходу передбачено метод, який включає використання першого набору з одного або більше вхідних параметрів шифру, щоб декодувати зашифровані дані в модулі протоколу отримання даних. У методі цього варіанту втілення винаходу кодовані дані були зашифровані із використанням другого набору з одного або більше вхідних параметрів шифру. Крім того, метод цього варіанту втілення винаходу включає порівняння параметрів принаймні частини декодованих даних із очікуваним значенням. Метод цього варіанту втілення винаходу також включає визначення виникнення помилки шифрування, коли параметри принаймні частини декодованих даних не дорівнюють очікуваним значенням. Метод цього варіанту втілення винаходу додатково включає ініціалізацію процедури повторної синхронізації шифрування у відповідь на визначення, що відбулася помилка шифрування, так щоб повторно синхронізувати принаймні один з першого набору вхідних параметрів шифру із

принаймні одним із другого набору вхідних параметрів шифру.

[0006] В іншому прикладі втілення винаходу передбачено апаратуру. Апаратура цього варіанту втілення винаходу включає принаймні один процесор та принаймні один запам'ятовуючий пристрій, що зберігає комп'ютерний програмний код, де принаймні один 5 запам'ятовуючий пристрій та збережений комп'ютерний програмний код, зконфігуровані принаймні з одним процесором, щоб змушувати апаратуру принаймні використовувати перший набір з одного або більше вхідних параметрів шифру для декодування зашифрованих даних в модулі протоколу отримання даних. В апаратурі цього варіанту втілення винаходу кодовані дані були зашифровані із використанням другого набору з одного або більше вхідних параметрів 10 шифру. Крім того, принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код, зконфігуровані принаймні з одним процесором, змушують апаратуру цього варіанту втілення винаходу порівнювати показники принаймні частини декодованих даних із очікуваним значенням. Принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код, зконфігуровані принаймні з одним процесором, додатково змушують апаратуру 15 цього варіанту втілення винаходу визначати виникнення помилки шифрування, коли параметри принаймні частини декодованих даних не дорівнюють очікуваному значенню. Принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код, зконфігуровані принаймні з одним процесором, також змушують апаратуру цього варіанту втілення винаходу ініціювати процедуру повторної синхронізації шифрування у відповідь на визначення, що відбулася помилка шифрування, так щоб повторно синхронізувати принаймні один з першого набору вхідних параметрів шифру із принаймні одним із другого набору вхідних параметрів шифру.

[0007] В іншому прикладі втілення винаходу передбачено комп'ютерний програмний продукт. Комп'ютерний програмний продукт включає принаймні один комп'ютерно-зчитуємий носій інформації, на якому зберігаються комп'ютерно-зчитуємі команди керуючої програми. Комп'ютерно-зчитуємі команди керуючої програми можуть включати велику кількість команд керуючої програми. Незважаючи на те, що в цьому короткому викладенні команди керуючої програми впорядковані, буде прийняте із вдячністю розуміння, що це резюме передбачене 25 лише з метою прикладу, та впорядкування повинне лише сприяти підведенню підсумків комп'ютерного програмного продукту. Приклад впорядкування жодним чином не обмежує реалізацію пов'язаних комп'ютерних команд керуючої програми. Перша команда керуючої програми цього варіанту втілення винаходу зконфігурована для використання першого набору з одного або більше вхідних параметрів шифру, щоб декодувати зашифровані дані в модулі протоколу отримання даних. Кодовані дані цього варіанту втілення винаходу були зашифровані 35 із використанням другого набору з одного або більше вхідних параметрів шифру. Друга команда керуючої програми цього варіанту втілення винаходу зконфігурована для порівняння параметрів принаймні частини декодованих даних із очікуваним значенням. Третя команда керуючої програми цього варіанту втілення винаходу зконфігурована для визначення виникнення помилки шифрування, коли параметри принаймні частини декодованих даних не дорівнюють очікуваному значенню. Четверта команда керуючої програми цього варіанту втілення винаходу зконфігурована для ініціювання процедури повторної синхронізації шифрування у відповідь на визначення, що відбулася помилка шифрування, так щоб повторно синхронізувати принаймні один з першого набору вхідних параметрів шифру із принаймні одним із другого набору вхідних параметрів шифру.

[0008] В іншому прикладі варіанту втілення винаходу передбачено апаратуру, що включає засоби для використання першого набору з одного або більше вхідних параметрів шифру для декодування зашифрованих даних в модулі протоколу отримання даних. Кодовані дані цього варіанту втілення винаходу були зашифровані із використанням другого набору з одного або 45 більше вхідних параметрів шифру. Крім того, апаратура цього варіанту втілення винаходу включає засоби для порівняння параметрів принаймні частини декодованих даних із очікуваним значенням. Апаратура цього варіанту втілення винаходу додатково включає засоби для визначення виникнення помилки шифрування, коли параметри принаймні частини декодованих даних не дорівнюють очікуваному значенню. Апаратура цього варіанту втілення винаходу також включає засоби для ініціювання процедури повторної синхронізації шифрування у відповідь на визначення, що відбулася помилка шифрування, так щоб повторно синхронізувати принаймні 50 один з першого набору вхідних параметрів шифру із принаймні одним із другого набору вхідних параметрів шифру.

[0009] Вищенаведене коротке викладення передбачене лише з метою розгляду деяких прикладів варіантів втілення винаходу для надання базового розуміння суті деяких аспектів винаходу. Відповідно, буде прийняте із вдячністю розуміння, що вищезгадані описані приклади 60

втілення винаходу є лише прикладами й не повинні тлумачитись, щоб будь-яким чином звузити обсяг або суть винаходу. Буде прийняте із вдячністю розуміння, що обсяг винаходу охоплює багато потенційних втілень винаходу, крім того, деякі з них, на додаток до тих, що були розглянуті, будуть описані нижче.

5       Короткий опис фігур

[0010] Маючи, у такий спосіб, описи варіантів втілення винаходу у загальних рисах, тепер будуть зроблені посилання до супровідних рисунків, які не обов'язково накреслено у масштабі, де:

10       [0011] Фіг. 1 ілюструє систему для виявлення помилок шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення даного винаходу;

[0012] Фіг. 2 є структурною блок-схемою мобільного термінала відповідно до типового варіанту втілення даного винаходу;

15       [0013] Фіг. 3 ілюструє схему послідовності операцій відповідно до типового методу для виявлення помилки шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення винаходу;

[0014] Фіг. 4 ілюструє схему послідовності операцій відповідно до типового методу для виявлення помилки шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення винаходу;

20       [0015] Фіг. 5 ілюструє схему послідовності операцій відповідно до типового методу для виявлення помилок шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення винаходу; та

[0016] Фіг. 6 ілюструє схему послідовності операцій відповідно до типового методу для виявлення помилок шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення винаходу.

25       Детальний опис

[0017] Деякі варіанти втілення даного винаходу тепер будуть описані в подальшому більш повно в цьому документі із посиланням до супровідних рисунків, у яких показані деякі, але не всі, варіанти втілення винаходу. Дійсно, винахід може бути реалізовано в багатьох різних формах, і не повинні розглядатися як обмежуючі варіанти втілення винаходу ті, що запропоновані тут; скоріше ці варіанти втілення винаходу надані так, щоб це розкриття задовольнило відповідні законні вимоги. Однакові цифрові посилання відсилають до однакових елементів на протязі всього документу.

35       [0018] Термін "схема", що тут використовується, відноситься до (а) реалізацій схеми тільки апаратними засобами (наприклад, реалізацій в аналоговій схемі й/або цифровій схемі); (b) комбінацій схем та комп'ютерного програмного продукту(ів), що включає програмне забезпечення й/або команди програмно-апаратних засобів, що зберігаються на одному або більше комп'ютерно-зчитуваних запам'ятовуваних пристроях, які спільно працюють, щоб змусувати апаратуру виконувати одну або більше описаних у цьому документі функцій; та (c) схеми, такі як, наприклад, мікропроцесор(и) або частина мікропроцесору(ів), які для роботи вимагають програмне забезпечення або програмно-апаратні засоби, навіть якщо програмне забезпечення або програмно-апаратні засоби фізично не присутні. Це визначення "схема" застосовується тут до всіх використань цього терміну, включаючи будь-які пункти формули винаходу. В подальшому прикладі, термін "схема", що тут використовується, також включає реалізацію, яка включає один або більше процесори й/або частину(и) нього й супровідне програмне забезпечення й/або програмно-апаратні засоби. Як інший приклад, термін "схема", що тут використовується, також включає, наприклад, інтегральну схему смуги частот модулюючих сигналів або інтегральну схему процесора пакетів для мобільного телефону або подібну інтегральну схему в сервері, пристрої стільникового зв'язку, інші мережеві пристрої, й/або інші обчислювальні пристрої.

50       [0019] Фіг. 1 ілюструє блок-схему системи 100 для виявлення помилки шифрування та відновлення безпомилкового стану відповідно до типового втілення даного винаходу. "Типовий" в значенні, що тут використовується, лише означає, що приклад як такий представляє один приклад варіанту втілення винаходу й не повинен розглядатися для звузування будь-яким чином обсягу або суті винаходу. Буде прийняте із вдячністю розуміння, що обсяг винаходу додатково до проілюстрованих і описаних у цьому документі охоплює багато потенційних втілень. По суті, у той час як Фіг. 1 ілюструє один приклад конфігурації системи для виявлення помилки шифрування та відновлення безпомилкового стану, багаточисленні інші конфігурації також можуть використовуватися, щоб забезпечити виконання варіантів втілення даного винаходу.

60       [0020] Принаймні в деяких варіантах втілення винаходу система 100 включає приймаючу

апаратуру 102, пов'язану з передаючою апаратурою 104 по мережі 108. Мережа 108 може включати бездротову мережу, дротову мережу або їх поєднання. В одному варіанті втілення винаходу, мережа 108 включає стільникову мережу або суспільно земельну мобільну мережу, такі, що можуть бути зконфігуровані для функціонування відповідно до стандартів Проекту

5 Партнерства Третього Покоління (3GPP). Мережа 108 може включати Інтернет.

[0021] Приймаючу апаратуру 102 може бути реалізовано як один або більше обчислювальних пристроїв. Наприклад, приймаючу апаратуру 102 може бути реалізовано як настільний комп'ютер, ноутбук, мобільний термінал, мобільний комп'ютер, мобільний телефон, пристрій мобільної комунікації, ігровий пристрій, цифрову камеру/відеокамеру, аудіо/відео

10 програвач, телевізійний пристрій, радіоприймач, цифровий відеоманітофон, пристрій позиціонування, будь-яке поєднання них, й/або подібних, зконфігуровані для одержання даних по мережі 108, які було зашифровано й/або передано передаючою апаратурою 104. Як інший приклад, приймаюча апаратура 102 може включати мережевий вузол (наприклад, контролер радіомережі (RNC), елемент керування мобільністю (MME), або подібні) зконфігурований для

15 декодування даних, переданих передаючою апаратурою 104, точку доступу (наприклад, базову станцію, вузол В, виокремлений вузол В, й/або іншу мережеву точку доступу), зконфігуровану для забезпечення доступу до мережі 108, одержання зашифрованих даних від передаючої апаратури 104, будь-який інший мережевий вузол, зконфігурований для виконання принаймні деяких функціональних можливостей, віднесених до передаючої апаратури 104 відповідно

20 цьому документу, деякі поєднання них, або подібних.

[0022] Аналогічно, передаючу апаратуру 104 може бути реалізовано як один або більше обчислювальні пристрої. Наприклад, передаючу апаратуру 104 може бути реалізовано як настільний комп'ютер, ноутбук, мобільний термінал, мобільний комп'ютер, мобільний телефон, пристрій мобільної комунікації, ігровий пристрій, цифрову камеру/відеокамеру, аудіо/відео

25 програвач, телевізійний пристрій, радіоприймач, цифровий відеоманітофон, пристрій позиціонування, будь-яке поєднання них, й/або подібних, зконфігуровані для шифрування й/або передання зашифрованих даних по мережі 108 до приймаючої апаратури 102. Як інший приклад, передаюча апаратура 104 може включати мережевий вузол (наприклад, контролер радіомережі (RNC), елемент керування мобільністю (MME), або подібні) зконфігурований для

30 шифрування даних для передачі на приймаючу апаратуру 102, точку доступу (наприклад, базову станцію, вузол В, виокремлений вузол В, й/або іншу мережеву точку доступу), зконфігуровану для забезпечення доступу до мережі 108 та передання зашифрованих даних до приймаючої апаратури 102, будь-який інший мережевий вузол, зконфігурований для виконання принаймні деяких функціональних можливостей, віднесених до передаючої апаратури 104

35 відповідно цьому документу, деякі поєднання них, або подібних.

У типовому варіанті втілення винаходу приймаючу апаратуру 102 й/або передаючу апаратуру 104 реалізовано як мобільний термінал, такий, як проілюстрований на Фіг. 2. В цьому відношенні, Фіг. 2 ілюструє блок-схему мобільного терміналу 10, представляючи один з

40 варіантів втілення приймаючої апаратури 102 й/або передаючої апаратури 104 відповідно до варіантів втілень даного винаходу. Однак потрібно мати на увазі, що мобільний термінал 10, проілюстрований та описаний нижче в цьому документі, лише ілюструє один тип приймаючої апаратури 102 й/або передаючої апаратури 104, який може здійснювати й/або мати переваги із втілень даного винаходу, й тому не повинен прийматися, щоб обмежити обсяг даного винаходу. У той час як декілька варіантів втілень електронного пристрою проілюстровані та будуть описані

45 нижче в цьому документі з метою прикладу, інші типи електронних пристроїв, таких як мобільні телефони, мобільні комп'ютери, портативні цифрові помічники (PDA), пейджери, ноутбуки, настільні комп'ютери, ігрові пристрої, телевізійні приймачі та інші типи електронних систем можуть використовувати втілення даного винаходу.

[0023] Як показано, мобільний термінал 10 може включати антену 12 (або множину антен

50 12), пов'язану з передавачем 14 та приймачем 16. Мобільний термінал 10 може також включати процесор 20, зконфігурований для надання сигналів до передавача та, відповідно, одержання сигналів від приймача. Процесор 20 може, наприклад, бути реалізованим як різноманітні засоби, що включають схему, один або більше мікропроцесорів із супровідним процесором(ами) цифрових сигналів, один або більше процесор(и) без супровідного процесора цифрових

55 сигналів, один або більше сопроцесорів, один або більше багатоядерних процесорів, один або більше контролерів, що обробляють схему, один або більше комп'ютерів, різні інші процесорні елементи, включаючи інтегральні схеми, такі як, наприклад, ASIC (прикладна інтегральна схема) або FPGA (вентильна матриця, що програмується в процесі експлуатації), або деякі них поєднання. Відповідно, незважаючи на те, що на Фіг. 2 проілюстровано одиночний процесор, у

60 деяких варіантах втілення винаходу процесор 20 включає множину процесорів. Ці сигнали,

передані та отримані процесором 20, можуть включати службове повідомлення відповідно до інтерфейсного стандарту ефіру відповідної стільникової системи, й/або будь-якої кількості різних дротових або бездротових мережевих технологій, включаючи, але не обмежуючись, технологіями Бездротової Точності (Wi-Fi), технологіями бездротової локальної мережі (WLAN), такими як 802.11, 802.16 Інституту Інженерів Електрики та Електроніки (IEEE), й/або подібними. Крім того, ці сигнали можуть включати мовні дані, сформовані користувачем дані, запитані користувачем дані, й/або подібні. В цьому відношенні, мобільний термінал може бути здатний до роботи з одним або більше інтерфейсними стандартами ефіру, комунікаційними протоколами, типами модуляції, типами доступу, й/або подібними. Більш того, мобільний термінал може бути здатний до роботи у відповідності до різних комунікаційних протоколів першого покоління (1G), другого покоління (2G), 2.5G, комунікаційних протоколів третього покоління (3G), комунікаційних протоколів четвертого покоління (4G), комунікаційних протоколів Підсистеми Передачі Мультимедійних Даних по IP-мережах (IMS), (наприклад, протоколів ініціювання сесії (SIP)), й/або подібних. Наприклад, мобільний термінал може бути здатний до роботи відповідно до 2G протоколів бездротового зв'язку IS-136 (Багатостанційного Доступу з Розділенням Каналів за Часом (TDMA)), Глобальної Системи Мобільних Комунікацій (GSM), IS-95 (Багатостанційного Доступу з Кодовим Розподілом Каналів (CDMA)), й/або подібних. Також, наприклад, мобільний термінал може бути здатний до роботи відповідно до протоколу бездротових комунікацій 2.5G Загального Пакетного Радіосервісу (GPRS), Поліпшених Даних GSM Середовища (EDGE), й/або подібних. Більш того, наприклад, мобільний термінал може бути здатний до роботи відповідно до 3G протоколів бездротового зв'язку, таких як Універсальної Мобільної Телекомунікаційної Системи (UMTS), Багатостанційного Доступу з Кодовим Розподілом Каналів 2000 (CDMA2000), Широкосмугового Множинного Доступу з Кодовим Поділом Каналів (WCDMA), Багатостанційного Доступу з Кодовим Поділом Каналів за Синхронним Режимом Поділу Часу (TD-SCDMA), й/або подібних. Мобільний термінал може, наприклад, бути сконфігурованим для передання й/або одержання даних, переданих відповідно до протоколу високошвидкісного пакетного передання даних по низхідній лінії зв'язку (HSDPA), до протоколу високошвидкісного пакетного передання даних по висхідній лінії зв'язку (HSUPA), й/або подібних. Мобільний термінал може бути додатково здатним до роботи відповідно до протоколів бездротового зв'язку 3.9G, таких як протокол Довгострокового Розвитку (LTE) або Розвиненої Мережі Універсального Наземного Радіодоступу (E-UTRAN) й/або подібних. Додатково, наприклад, мобільний термінал може бути здатний до роботи відповідно до протоколів бездротового зв'язку четвертого покоління (4G) й/або подібних, а також подібних протоколів бездротового зв'язку, які можуть бути розроблені в майбутньому.

[0024] Також можуть використовувати переваги із втілень цього винаходу певні мобільні термінали Вузкосмугових Вдосконалених Мобільно-Телефонних Систем (NAMPS), так само як Загальнодоступних Комунікаційних Систем (TACS), як повинні використовувати переваги із втілень цього винаходу телефони з подвійним або вище режимом (наприклад, цифрові/аналогові або TDMA/CDMA/аналогові телефони). Додатково, мобільний термінал 10 може бути здатний до роботи відповідно до протоколів Wireless Fidelity (Wi-Fi) або Міжнародної Взаємодії у Мікрохвильовому Діапазоні Доступу (WiMAX).

[0025] Було обумовлено, що процесор 20 може включати схему для здійснення аудіо/відео та логічних функцій мобільного терміналу 10. Наприклад, процесор 20 може включати пристрій процесору цифрових сигналів, пристрій мікропроцесору, аналого-цифровий конвертер, цифро-аналоговий конвертер, й/або подібні. Функції керування й обробки сигналу мобільного терміналу можуть бути розподілені між цими пристроями відповідно до їхніх відповідних можливостей. Процесор може додатково включати внутрішній голосовий кодер-декодер (VC) 20a, внутрішній модем даних (DM) 20b, й/або подібні. Крім того, процесор 20 може включати функціональні можливості керувати однією або більше програмами, які можуть зберігатися у запам'ятовуючому пристрої. Наприклад, процесор 20 може бути здатний до роботи з програмою забезпечення зв'язку, такою як web-браузер. Програма забезпечення зв'язку може дозволити мобільному терміналу 10 передавати й одержувати веб-контент, такий як локалізований контент, відповідно до протоколу, такому як Протокол Бездротових Прикладних Програм (WAP), протокол передачі гіпертексту (HTTP), й/або подібні. Мобільний термінал 10 може бути здатний до використання Протоколу Керування Передачею/Internet Протоколом (TCP/IP) для передання та отримання веб-контенту через Інтернет або інші мережі.

[0026] Мобільний термінал 10 може також містити інтерфейс користувача, що включає, наприклад, навушник або динамік 24, дзвінок 22, мікрофон 26, дисплей 28, інтерфейс введення даних користувача, й/або подібні, які можуть бути функціонально поєднані із процесором 20. В цьому відношенні, процесор 20 може включати схему інтерфейсу користувача, сконфігуровану

для керування принаймні деякими функціями або елементами інтерфейсу користувача, такими як, наприклад, динамік 24, дзвінок 22, мікрофон 26, дисплей 28, й/або подібні. Процесор 20 й/або схема інтерфейсу користувача, що включає процесор 20, можуть бути зконфігуровані для керування однією або більше функціями одного або більше елементів інтерфейсу користувача через команди комп'ютерної програми (наприклад, програмного забезпечення й/або програмно-апаратних засобів), що зберігаються на запам'ятовуючому пристрої, доступному для процесора 20 (наприклад, енергозалежному запам'ятовуючому пристрої 40, енергонезалежному запам'ятовуючому пристрої 42, й/або подібному). Незважаючи на те, що це не розглянуто, мобільний термінал може включати батарею для живлення різних схем, пов'язаних з мобільним терміналом, наприклад, схеми для забезпечення механічної вібрації, що виявляється на виході. Вхідний інтерфейс користувача може включати пристрої, що дозволяють мобільному терміналу одержати дані, такі як клавіатура 30, сенсорний дисплей (не показаний), джойстик (не показаний), й/або інший пристрій введення даних. Варіанти втілення винаходу включають клавіатуру, клавіатура може включати цифрові (0-9) та пов'язані клавіші (#, \*), й/або інші клавіші для того, щоб управляти мобільним терміналом.

[0027] Як показано на Фіг. 2, мобільний термінал 10 може також включати один або більше засобів для спільного використання й/або одержання даних. Наприклад, мобільний термінал може включати приймач-передавач короткого діапазону радіочастот (RF) й/або пристрій опитування 64, так що дані можуть бути спільно використовуватись з й/або бути отримані від електронних пристроїв відповідно до обладнання RF. Мобільний термінал може включати інші приймачі-передавачі короткого діапазону, такі як, наприклад, інфрачервоний приймач-передавач (IR) 66, приймач-передавач 68 Bluetooth™ (BT), який при експлуатації використовує бездротову технологію під знаком товарів та послуг Bluetooth™, розроблену Професійною Групою Bluetooth™, бездротовий приймач-передавач 70 універсальної послідовної шини (USB) й/або подібні. Приймач-передавач 68 технології Bluetooth™ може бути здатний до роботи відповідно до радіо стандартів ультра-малої потужності технології Bluetooth™ (наприклад, Wibree™). В цьому відношенні, мобільний термінал 10 та, зокрема, приймач-передавач короткого діапазону може бути здатний до передачі даних до й/або одержання даних від електронних пристроїв у межах просторової близькості від мобільного терміналу, наприклад, у межах 10 метрів. Незважаючи на те, що це не розглянуто, мобільний термінал може бути здатний до передачі й/або одержання даних від електронних пристроїв відповідно до різних бездротових мережних технологій, включаючи технологію Бездротової Точності (Wi-Fi), технології WLAN, такі як технологія IEEE 802.11, технологія IEEE 802.16, й/або подібні.

[0028] Мобільний термінал 10 може включати запам'ятовуючий пристрій, такий як модуль ідентифікації абонента (SIM) 38, змінний модуль ідентифікації користувача (R-UIM), універсальний модуль ідентифікації абонента (USIM), й/або подібні, який може зберігати інформаційні елементи, пов'язані з мобільним абонентом. Додатково із SIM, мобільний термінал може включати інший змінний й/або встановлений запам'ятовуючий пристрій. Мобільний термінал 10 може включати енергозалежний запам'ятовуючий пристрій 40 й/або енергонезалежний запам'ятовуючий пристрій 42. Наприклад, енергозалежний запам'ятовуючий пристрій 40 може містити оперативну пам'ять (RAM) включаючи динамічну й/або статичну RAM, внутрішню кеш-пам'ять або кеш другого рівня, й/або подібну. Енергонезалежний запам'ятовуючий пристрій 42, що може бути вбудований й/або змінний, може включати, наприклад, постійний запам'ятовувальний пристрій, флеш-пам'ять, магнітні запам'ятовувальні пристрої (наприклад, жорсткі диски, накопичувачі на гнучких магнітних дисках, магнітні стрічки, і т.д.), приводи оптичних дисків й/або засоби аудіовізуальної інформації, енергонезалежну оперативну пам'ять (NVRAM), й/або подібне. Подібно енергозалежному запам'ятовуючому пристрою 40 енергонезалежний запам'ятовуючий пристрій 42 може включати кеш-область для тимчасового зберігання даних. Блоки запам'ятовуючих пристроїв можуть зберігати одну або більше програм, команди, елементи інформації, дані, й/або подібне, що може використовуватись мобільним терміналом для того, щоб виконувати функції мобільного терміналу. Наприклад, блоки запам'ятовуючих пристроїв можуть включати ідентифікатор, такий як код міжнародного ідентифікатора мобільного обладнання (IMEI), здатний до однозначного визначення мобільного терміналу 10.

[0029] Повертаючись тепер до Фіг. 1, у типовому втіленні винаходу приймаюча апаратура 102 включає різні засоби, такі як процесор 110, запам'ятовуючий пристрій 112, комунікаційний інтерфейс 114, та схему керування дешифруванням 118 для того, щоб виконувати різні функції, які тут описані. Ці засоби приймаючої апаратури 102, як описано в цьому документі, можуть бути втілені як, наприклад, схема, апаратні елементи (наприклад, відповідно запрограмований процесор, комбінаційна логічна схема, й/або подібні), комп'ютерний програмний продукт, що



включає програмні команди, що зчитуються комп'ютером (наприклад, програмне забезпечення або програмно-апаратні засоби), які зберігаються на засобах, що зчитуються комп'ютером (наприклад, запам'ятовуючому пристрої 112), що виконуються відповідно зконфігурованим пристроєм обробки (наприклад, процесором 110), або деяким поєднанням них.

5 [0030] Процесор 110 може, наприклад, бути реалізованим як різні засоби, включаючи один або більше мікропроцесорів із супроводжувальним процесором(ами) цифрових сигналів, один або більше процесор(ів) без супроводжувального процесору цифрових сигналів, один або більше сопроцесорів, один або більше багатоядерних процесорів, один або більше контролерів, обробляючих схему, один або більше комп'ютерів, різні інші процесорні елементи, включаючи  
10 інтегральні схеми, такі як, наприклад, ASIC (спеціалізовані інтегральні схеми) або FPGA (вентильна матриця, що програмується користувачем), або деяке поєднання них. Відповідно, незважаючи на те, що на Фіг. 1 проілюстровано одиночний процесор, у деяких варіантах втіленнях винаходу процесор 110 включає багато процесорів. Багато процесорів можуть перебувати у функціональній взаємодії один з іншим та можуть бути всі разом зконфігуровані  
15 для виконання однієї або більше функціональних можливостей приймаючої апаратури 102, як описано у цьому документі. Багато процесорів можуть бути об'єднані у єдиний обчислювальний пристрій або розподілені на багато обчислювальних пристроїв, що усі разом зконфігуровані для виконання однієї або більше функціональних можливостей приймаючої апаратури 102, як описано у цьому документі. У втіленнях винаходу, де приймаючу апаратуру 102 реалізовано як  
20 мобільний термінал 10, процесор 110 може бути реалізований як процесор 20, або включати процесор 20. У типовому втіленні винаходу процесор 110 зконфігурований для виконання команд, які зберігаються в запам'ятовуючому пристрої 112 або інакше доступні для процесора 110. Коли ці команди виконуються процесором 110, це може змушувати приймаючу апаратуру 102 виконувати одну або більше функціональних можливостей приймаючої апаратури 102, як  
25 описано у цьому документі. Також, зконфігурований або апаратними, або програмними методами, або поєднанням них, процесор 110 може включати відповідно зконфігурований об'єкт, здатний до виконання операцій відповідно до варіантів втілення даного винаходу. Таким чином, наприклад, коли процесор 110 реалізовано як ASIC, FPGA або подібні, процесор 110 може включати особливо зконфігуровані апаратні засоби для того, щоб провести одну або  
30 більше операцій, описаних у цьому документі. Альтернативно, як інший приклад, коли процесор 110 реалізовано як пристрій, що виконує програмні команди, які можуть бути збережені в запам'ятовуючому пристрої 112, команди можуть особливо конфігурувати процесор 110 для виконання одного або більше алгоритмів і операцій, описаних у цьому документі.

[0031] Запам'ятовуючий пристрій 112 може включати, наприклад, енергозалежний й/або енергонезалежний запам'ятовуючий пристрій. Незважаючи на те, що на Фіг. 1 проілюстрований єдиний запам'ятовуючий пристрій, запам'ятовуючий пристрій 112 може включати багато блоків пам'яті. Запам'ятовуючий пристрій 112 може включати енергозалежний запам'ятовуючий пристрій, енергонезалежний запам'ятовуючий пристрій, або деяку їх комбінацію. В цьому  
35 відношенні, запам'ятовуючий пристрій 112 може включати, наприклад, жорсткий диск, оперативну пам'ять, кеш-пам'ять, флеш-пам'ять, носій компакт-диску тільки для зчитування (CD-ROM), цифровий багатоцільовий диск тільки для зчитування (DVD-ROM), оптичний диск, схему, зконфігуровану для зберігання інформації, або деяку їх комбінацію. У втіленнях, де приймаючу апаратуру 102 реалізовано як мобільний термінал 10, запам'ятовуючий пристрій 112 може включати енергозалежний запам'ятовуючий пристрій 40 й/або енергонезалежний  
40 запам'ятовуючий пристрій 42. Запам'ятовуючий пристрій 112 може бути зконфігурований для зберігання інформації, даних, прикладних програм, команд, або подібного для того, щоб дати можливість приймаючій апаратурі 102 виконувати різні функції відповідно до типових втілень даного винаходу. Наприклад, принаймні в деяких варіантах втілення винаходу, запам'ятовуючий пристрій 112 зконфігурований для буферизування вхідних даних для  
45 оброблення процесором 110. Додатково або альтернативно, принаймні в деяких втіленнях, запам'ятовуючий пристрій 112 зконфігурований для зберігання програмних команд для виконання процесором 110. Запам'ятовуючий пристрій 112 може зберігати інформацію у формі статичної й/або динамічної інформації. Ця інформація, що зберігається, може бути збережена й/або використана схемою керування дешифруванням 118 протягом виконання її  
50 функціональних можливостей.

[0032] Комунікаційний інтерфейс 114 може бути реалізовано як будь-який пристрій або засоби, втілені в схему, апаратні засоби, комп'ютерний програмний продукт, що включає програмні команди, що зчитуються комп'ютером, які зберігаються на засобі, що зчитується комп'ютером (наприклад, запам'ятовуючому пристрої 112), та виконуються пристроєм обробки  
60 (наприклад, процесором 110), або їх поєднання, що зконфігуровані для одержання й/або

передачі даних від/до об'єкту системи 100, такого як, наприклад, передаюча апаратура 104. Принаймні в одному втіленні винаходу комунікаційний інтерфейс 114 принаймні частково реалізований як процесор 110 або ж управляється процесором 110. В цьому відношенні, комунікаційний інтерфейс 114 може бути у взаємодії із процесором 110, наприклад через шину.

5 Комунікаційний інтерфейс 114 може включати, наприклад, антену, передавач, приймач, приймач-передавач й/або підтримуючі апаратні засоби або програмне забезпечення для того, щоб допустити зв'язки з одним або більше об'єктом системи 100. Комунікаційний інтерфейс 114 може бути зконфігурований для одержання й/або передачі даних, використовуючи будь-який протокол, який може використовуватися для зв'язку між об'єктами системи 100. Комунікаційний

10 інтерфейс 114 може додатково бути у взаємодії з пам'яттю 112 й/або схемою керування дешифруванням 118, наприклад, через шину.

[0033] Схема керування дешифруванням 118 може бути реалізована як різні засоби, такі як схема, апаратні засоби, комп'ютерний програмний продукт, що включає програмні команди, що зчитуються комп'ютером, які зберігаються на засобі, що зчитується комп'ютером

15 (наприклад, запам'ятовуючому пристрої 112), та виконуються пристроєм обробки (наприклад, процесором 110), або їх поєднанням, й, в одному втіленні винаходу, реалізована як процесор 110 або ж управляється процесором 110. У варіанті втілення винаходу, де схема керування дешифруванням 118 втілена окремо від процесора 110, схема керування дешифруванням 118 може бути у взаємодії із процесором 110. Схема керування дешифруванням 118 може включати

20 й/або бути зконфігурована для виконання принаймні деяких функціональних можливостей керування об'єктом радіоканалу (RLC), об'єктом протоколу конвергенції пакетних даних (PDCP), й/або подібних. Схема керування дешифруванням 118 може, крім того, бути у взаємодії з одним або більше запам'ятовуючих пристроїв 112 або комунікаційним інтерфейсом 114, наприклад, через шину.

[0034] Посилаючись тепер до передаючої апаратури 104, у типовому варіанті втілення винаходу передаюча апаратура 104 включає різні засоби, такі як процесор 120, запам'ятовуючий пристрій 122, комунікаційний інтерфейс 124 та схему керування шифруванням 126 для того, щоб виконувати різні функції, описані в цьому документі. Ці засоби передаючої апаратури 104, як описано в цьому документі, можуть бути втілені як, наприклад, схема,

30 апаратні елементи (наприклад, відповідно запрограмований процесор, комбінаційна логічна схема, й/або подібні), комп'ютерний програмний продукт, що включає програмні команди, що зчитуються комп'ютером (наприклад, програмне забезпечення або програмно-апаратні засоби), збережені на засобі, що зчитується комп'ютером (наприклад, запам'ятовуючому пристрої 122), що виконується відповідно зконфігурованим пристроєм обробки (наприклад,

35 процесором 120), або деяким них поєднанням.

[0035] Процесор 120 може, наприклад, бути реалізованим як різноманітні засоби, один або більше мікропроцесорів із супровідним процесором(ами) цифрових сигналів, один або більше процесор(и) без супровідного процесора цифрових сигналів, один або більше сопроцесорів, один або більше багатоядерних процесорів, один або більше контролерів, що обробляють

40 схему, один або більше комп'ютерів, різні інші процесорні елементи включаючи інтегральні схеми, такі як, наприклад, ASIC (прикладна інтегральна схема) або FPGA (вентильна матриця, що програмується в процесі експлуатації), або деяким них поєднанням. Відповідно, незважаючи на те, що на Фіг. 1 проілюстровано одиночний процесор, у деяких варіантах втілення винаходу процесор 120 включає багато процесорів. Багато процесорів можуть бути у функціональній

45 взаємодії один з одним та можуть бути зконфігуровані всі разом, щоб виконувати одну або більше функціональних можливостей передаючої апаратури 104, як описано у цьому документі. Багато процесорів може бути реалізовані на єдиному обчислювальному пристрої або розподілені на багато обчислювальних пристроїв, усі разом зконфігурованих для виконання однієї або більше функціональних можливостей передаючої апаратури 104, як описано у цьому

50 документі. У втіленнях, де передаюча апаратура 104 реалізована як мобільний термінал 10, процесор 120 може бути реалізований як процесор 20 або включати процесор 20. У типовому втіленні процесор 120 зконфігурований для виконання команд, збережених в запам'ятовуючому пристрої 122 або інакше доступних процесору 120. Коли ці команди виконуються процесором 120, це може змушувати передаючу апаратуру 104 виконувати одну

55 або більше функціональних можливостей передаючої апаратури 104, як описано у цьому документі. Також, чи зконфігуровану апаратними, або програмними методами, або ж їх комбінацією, процесор 120 може включати об'єкт, здатний, відповідно зконфігурований, до виконання операцій відповідно до варіантів втілення даного винаходу. Таким чином, наприклад, коли процесор 120 реалізовано як ASIC, FPGA або подібне, процесор 120 може включати

60 особливо зконфігуровані апаратні засоби для того, щоб проводити одну або більше операцій,

описаних у цьому документі. Альтернативно, як інший приклад, коли процесор 120 реалізовано як виконувач командних програм, тих, які можуть бути збережено в запам'ятовуючому пристрої 122, команди можуть особливо конфігурувати процесор 120 для виконання одного або більше описаних у цьому документі алгоритмів і операцій.

5 [0036] Запам'ятовуючий пристрій 122 може включати, наприклад, енергозалежну й/або енергонезалежну пам'ять. Незважаючи на те, що на Фіг. 1 проілюстрований єдиний запам'ятовуючий пристрій, запам'ятовуючий пристрій 122 може включати багато блоків пам'яті. Багато блоків пам'яті можуть бути реалізовані на єдиному обчислювальному пристрої або розподілені на багато обчислювальних пристроїв. Запам'ятовуючий пристрій 122 може

10 включати енергозалежну пам'ять, енергонезалежну пам'ять, або деяке їхнє поєднання.  
В цьому відношенні, запам'ятовуючий пристрій 122 може включати, наприклад, жорсткий диск, оперативну пам'ять, кеш-пам'ять, флеш-пам'ять, носій компакт-диску тільки для зчитування (CD-ROM), цифровий багатоцільовий диск тільки для зчитування (DVD-ROM), оптичний диск, схему, зконфігуровану для зберігання інформації, або деяку них комбінацію. У

15 варіантах втілення винаходу, де передаючу апаратуру 104 реалізовано як мобільний термінал 10, запам'ятовуючий пристрій 122 може включати енергозалежний запам'ятовуючий пристрій 40 й/або енергонезалежний запам'ятовуючий пристрій 42. Запам'ятовуючий пристрій 122 може бути зконфігурований для зберігання інформації, даних, прикладних програм, команд, або подібного для того, щоб дати можливість передаючій апаратурі 104 виконувати різні функції

20 відповідно до типових втілень даного винаходу. Наприклад, принаймні в деяких втіленнях, запам'ятовуючий пристрій 122 зконфігурований для буферизування вхідних даних для оброблення процесором 120. Додатково або альтернативно, принаймні в деяких втіленнях, запам'ятовуючий пристрій 122 зконфігурований для зберігання програмних команд для виконання процесором 120. Запам'ятовуючий пристрій 122 може зберігати інформацію у формі статичної й/або динамічної інформації. Ця інформація, що зберігається, може бути збережена

25 й/або використана схемою керування шифруванням 126 протягом виконання її функціональних можливостей.

[0037] Комунікаційний інтерфейс 124 може бути реалізовано як будь-який пристрій або засоби, втілені в схему, апаратні засоби, комп'ютерний програмний продукт, що включає

30 програмні команди, що зчитуються комп'ютером, які зберігаються на засобі, що зчитується комп'ютером (наприклад, запам'ятовуючому пристрої 122), та виконуються пристроєм обробки (наприклад, процесором 120), або їх поєднання, що зконфігуровано для одержання й/або передачі даних від/до об'єкту системи 100, такого як, наприклад, приймаюча апаратура 102. Принаймні в одному варіанті втілення винаходу комунікаційний інтерфейс 124 принаймні

35 частково реалізовано як процесор 120 або ж управляється процесором 120. В цьому відношенні, комунікаційний інтерфейс 124 може бути у взаємодії із процесором 120, наприклад, через шину. Комунікаційний інтерфейс 124 може включати, наприклад, антену, передавач, приймач, приймач-передавач й/або підтримуючі апаратні засоби або програмне забезпечення для того, щоб допустити зв'язки з одним або більше об'єктом системи 100. Комунікаційний

40 інтерфейс 124 може бути зконфігурований для одержання й/або передачі даних, використовуючи будь-який протокол, який може використовуватися для зв'язку між об'єктами системи 100. Комунікаційний інтерфейс 124 може додатково бути у взаємодії з пам'яттю 122 й/або схемою керування кодування 126, наприклад, через шину.

[0038] Схема керування шифруванням 126 може бути реалізована як різні засоби, такі як

45 схема, апаратні засоби, комп'ютерний програмний продукт, що включає програмні команди, що зчитуються комп'ютером, які зберігаються на засобі, що зчитується комп'ютером (наприклад, запам'ятовуючому пристрої 122), та виконуються пристроєм обробки (наприклад, процесором 120), або поєднання цього, та, в одному варіанті втілення винаходу, реалізована як процесор 120 або ж управляється процесором 120. У варіанті втілення винаходу, де схема

50 керування шифруванням 126 реалізована окремо від процесора 120, схема керування шифруванням 126 може бути у взаємодії із процесором 120. Схема керування шифруванням 126 може включати засоби й/або бути зконфігурована для виконання принаймні деякі функціональні можливості об'єкту RLC, об'єкту PDCCP, й/або подібних. Схема керування шифруванням 126 може, крім того, бути у взаємодії з одним або більше запам'ятовуючим

55 пристроєм 122 або комунікаційним інтерфейсом 124, наприклад, через шину.

[0039] Буде прийняте із вдячністю розуміння, що в деяких варіантах втілення винаходу приймаюча апаратура 102 зконфігурована для виконання принаймні деяких з функціональних можливостей передаючої апаратури 104, як описано у цьому документі. В цьому відношенні, приймаюча апаратура 102 може включати схему керування шифруванням 126, яка може бути

60 реалізована як процесор 110 або ж управлятися процесором 110.

Аналогічним образом, в деяких втіленнях передаюча апаратура 104 сконфігурована для виконання принаймні деяких з функціональних можливостей приймаючої апаратури 102, як описано у цьому документі. В цьому відношенні, передаюча апаратура 104 може включати схему керування дешифруванням 118, яка може бути реалізована як процесор 120 або ж управлятися процесором 120. Відповідно, варіанти втілення винаходу можуть полегшити виявлення помилок шифрування й відновлення безпомилкового стану як у мережному висхідному каналі зв'язку, так і у мережному низхідному каналі зв'язку.

[0040] Схема керування шифруванням 126 сконфігурована в деяких варіантах втілення винаходу, щоб шифрувати дані в модулі протоколу даних (PDU), який повинен бути переданий на приймаючу апаратуру 102. PDU може включати RLC PDU, PDCP PDU, або подібні. PDU може включати режим непідтвердження (UM) PDU таким чином, щоб приймаюча апаратура 102 не була зобов'язана підтверджувати одержання UM PDU. Альтернативно, PDU може включати режим підтвердження (AM) PDU таким чином, щоб приймаюча апаратура 102 була зобов'язана підтверджувати одержання PDU. PDU може бути пов'язаний з будь-яким з розмаїття типів сервісу комунікаційного обміну між приймаючою апаратурою 102 та передаючою апаратурою 104 або іншим пристроєм у мережі 108. Тип сервісу включає більш високий рівень комунікаційної прикладної програми, яка підтримується модулем(ями) PDU, що передаються на приймаючу апаратуру 102. Наприклад, тип сервісу може включати голосову комунікацію комутації каналів (CS), передану по Високошвидкісному Пакетному Доступу (HSPA). В іншому прикладі тип сервісу може включати мовний сигнал по Internet-протоколу (VoIP), потоковий сервіс, або інший сервіс реального часу. Схема керування шифруванням 126 може бути сконфігурована для шифрування даних, використовуючи набір з одного або більше вхідних параметрів шифру. Набір з одного або більше вхідних параметрів шифру може включати, наприклад, один або більше ключів шифрування (СК), COUNT-C, BEARER (наприклад, радіо-ідентифікаційні дані несучої), LENGTH (наприклад, довжина параметру DATA), DATA (наприклад, параметр даних, які будуть зашифровані), або подібні. Значення COUNT-C може включати й/або бути визначене базуючись принаймні частково на гіперфреймовому номері (HFN) та порядковому номері (наприклад, порядковому номері RLC (RLC SN)). HFN може включати поле, ініціалізоване на початкове значення, обмінюване між передаючою апаратурою 104 та приймаючою апаратурою 102 під час настроювання радіо-несучої. RLC SN може включати порядковий номер, включений у заголовок PDU, що може бути збільшений на 1 при кожній передачі PDU. Схема керування шифруванням 126 може використовувати набір вхідних параметрів шифру, щоб шифрувати дані, використовуючи будь-який кодер-декодер, такий як, наприклад, кодер-декодер Адаптивного Мультирівня (AMR), Широкосмуговий-AMR (AMR-WM), й/або подібні.

[0041] Схема керування шифруванням 126 може бути попередньо сконфігурована, щоб включати зашифроване "очікуване значення" в PDU, який буде переданий на приймаючу апаратуру 102. Очікуване значення може включати значення додаткового поля, індикатору довжини, заголовку PDU, поле, яке тепер визначене як поле R (наприклад, в PDCP PDU), й/або інші значення. Наприклад, додаткове поле може включати один або більше бітів, що мають значення, очікуване приймаючою апаратурою 102, що включено в PDU, щоб передбачити синхронізацію по октету даних у межах PDU. В іншому прикладі індикатор довжини може вказувати останній октет кожного RLC сервісного модулю даних, включеного в PDU (наприклад, "1111101" для CS мовного сигналу по HSPA). Таким чином, очікуване значення може вказувати розмір PDU або інше значення, очікуване приймаючою апаратурою 102. У ще одному прикладі заголовок PDU може включати значення, що вказує тип PDCP, з яким пов'язаний PDCP PDU (наприклад, "010" PDCP AMR Дані PDU для CS мовного сигналу по HSPA, "000" PDCP Дані PDU для VoIP, й/або подібні).

[0042] У деяких втіленнях "очікуване значення" попередньо визначене, базуючись на конфігурації системи 100. Додатково або альтернативно, схема керування шифруванням 126 і схема керування дешифруванням 118 можуть бути сконфігуровані, щоб незалежно визначати очікуване значення, базуючись принаймні частково на типі комунікаційного сервісу, для якого дані обмінюються між приймаючою апаратурою 102 та передаючою апаратурою 104 (наприклад, очікуване значення заголовку PDU). В іншому прикладі схема керування шифруванням 126 може бути сконфігурована для визначення очікуваного значення й забезпечення очікуваним значенням приймаючу апаратуру 102 під час фази настроювання комунікації (наприклад, під час настроювання радіо-несучої, під час повторної синхронізації RLC, й/або подібного).

[0043] Як тільки PDU, включаючи значення, очікуване приймаючою апаратурою 102, зашифроване, комунікаційний інтерфейс 124 може передати PDU на приймаючу апаратуру 102,

де він може бути отриманий інтерфейсом комунікації 114. В деяких варіантах втілення винаходу схема керування дешифруванням 118 сконфігурована для використання набору з одного або більше вхідних параметрів шифру, що обслуговуються схемою керування дешифруванням 118, щоб декодувати зашифровані дані в отриманому PDU.

Набір з одного або більше вхідних параметрів шифру може включати, наприклад, один або більше ключів шифрування (СК), COUNT-C, BEARER (наприклад, радіо-ідентифікаційні дані несучої), LENGTH (наприклад, довжина параметру DATA), DATA (наприклад, параметр даних, які будуть дешифровані), або подібні. Схема керування дешифруванням 118 може бути сконфігурована для використання набору вхідних параметрів шифру для того, щоб дешифрувати дані, використовуючи будь-який кодер-декодер, що був використаний схемою керування шифруванням 126 для шифрування даних.

[0044] Після того, як схема керування дешифруванням 118 декодувала зашифровані дані, в деяких варіантах втілення винаходу схема керування дешифруванням 118 сконфігурована для порівнювання значення принаймні частини декодованих даних із очікуваним значенням. Як описано вище, очікуване значення, очікуване схемою керування дешифруванням 118, може бути попередньо сконфігуроване, обране схемою керування шифруванням 126 і визначене схемою керування дешифруванням 118 базуючись принаймні частково на інформації мережевій передачі сигналів, отриманої терміналом 102, визначене схемою керування дешифруванням 118 базуючись принаймні частково на типі сервісу, з яким пов'язаний отриманий PDU, й/або подібне. Принаймні частина декодованих даних може включати частину (наприклад, заголовок, поле, й/або подібне) PDU, у якому розташовано очікуване значення. Коли значення принаймні частини декодованих даних не дорівнює очікуваному значенню, в деяких варіантах втілення винаходу схема керування дешифруванням 118 сконфігурована для визначення виникнення помилки шифрування. В цьому відношенні, якщо набір вхідних параметрів шифрування, використовуваних схемою керування дешифруванням 118 для декодування даних, синхронізований з набором вхідних параметрів шифрування, використовуваних схемою керування шифруванням 126 для шифрування даних, принаймні частина декодованих даних повинна рівнятися очікуваному значенню.

[0045] В деяких варіантах втілення винаходу схема керування дешифруванням 118 сконфігурована для ініціювання процедури повторної синхронізації шифрування у відповідь на визначення, що відбулася помилка шифрування, щоб повторно синхронізувати принаймні один з набору вхідних параметрів шифру, використовуваних схемою керування дешифруванням 118 для декодування зашифрованих даних в отриманому PDU ("перший набір вхідних параметрів шифру") принаймні із одним з набору вхідних параметрів шифру, використаних схемою керування шифруванням 126 для шифрування даних в PDU, переданому на приймаючу апаратуру 102 ("другий набір вхідних параметрів шифру"). В цьому відношенні, повторна синхронізація принаймні одного з першого набору вхідних параметрів шифру принаймні із одним із другого набору вхідних параметрів шифру може включати, наприклад, незалежне оновлення схемою керування дешифруванням 118 одного або більше вхідних параметрів шифру першого набору, оновлення схемою керування дешифруванням 118 одного або більше вхідних параметрів шифру першого набору базуючись на інформації обміну сигналами з передаючою апаратурою 104, встановлення схемою керування дешифруванням 118 та схемою керування шифруванням 126 однієї і тієї ж передаючої апаратури 104 одного або більше синхронізованих вхідних параметрів шифру для перших і других наборів у фазі настроювання (наприклад, настроювання радіо-несучої й/або командна процедура режиму безпеки), й/або встановлення схемою керування дешифруванням 118 та схемою керування шифруванням 126 з різної передаючої апаратури 104 одного або більше синхронізованих вхідних параметрів шифру для перших і других наборів у фазі настроювання (наприклад, настроювання несучої, реконфігурування радіо-несучої, й/або командна процедура режиму безпеки).

[0046] У деяких варіантах втілення винаходу схема керування дешифруванням 118 сконфігурована для ініціювання процедури повторної синхронізації шифрування шляхом ініціювання процедури повторної синхронізації RLC (наприклад, процедури повторного встановлення RLC при експлуатації в режимах UM або AM, процедури перенастроювання RLC при експлуатації в режимі AM, й/або подібних), щоб ініціалізувати принаймні один вхідний параметр шифру таким чином, щоб перший набір вхідних параметрів шифру був повторно синхронізований із другим набором вхідних параметрів шифру. В цьому відношенні, приймаюча апаратура 102 та передаюча апаратура 104 можуть брати участь у процедурі корекції ячейки й схема керування дешифруванням 118 та схема керування шифруванням 126 можуть ініціювати повторне встановлення RLC або іншу процедуру повторної синхронізації RLC як частину процедури корекції ячейки так, щоб схема керування дешифруванням 118 і схема керування

шифруванням 126 могли ініціалізувати принаймні один синхронізований вхідний параметр шифру (наприклад, значення COUNT-C, UM RLC SN, й/або подібні).

[0047] Додатково або альтернативно, у деяких втіленнях, схема керування дешифруванням 118 зконфігурована для ініціювання автономної процедури повторної синхронізації шифрування. В цьому відношенні, схема керування дешифруванням 118 може бути зконфігурована для вибирання найбільш вірогідного альтернативного значення для принаймні одного з першого набору вхідних параметрів шифру. Найбільш вірогідне альтернативне значення може, наприклад, включати збільшене значення вхідного параметру шифру, коли вхідний параметр шифру включає параметр, який збільшується при кожному одержанні PDU. Наприклад, схема керування дешифруванням може бути зконфігурована для збільшення значення HFN COUNT-C до поточного значення HFN COUNT-C + 1 як найбільш вірогідного альтернативного значення. Тоді схема керування дешифруванням 118 може використовувати обране найбільш вірогідне альтернативне значення для принаймні одного з першого набору вхідних параметрів шифру, щоб декодувати дані в отриманому PDU, для якого відбулася помилка шифрування або декодувати дані у пізніше отриманому PDU. Якщо обране принаймні одне найбільш вірогідне альтернативне значення для вхідного параметру(ів) шифру є правильно синхронізованим значенням(и), то принаймні частина декодованих даних буде дорівнювати очікуваним значенням. Якщо принаймні частина декодованих даних не дорівнює очікуваним значенням, то перші й другі набори вхідних параметрів шифру усе ще не синхронізовані, і схема керування дешифруванням 118 може бути зконфігурована, щоб знову вибирати найбільш вірогідне альтернативне значення для одного або більше вхідних параметрів шифру та знову спробувати декодувати отриманий PDU. Схема керування дешифруванням 118 може бути зконфігурована для повторення процесу вибору самої вірогідної альтернативи для одного або більше вхідних параметрів шифру до тих пір, коли схема керування дешифруванням 118 автономно повторно синхронізує принаймні один параметр першого набору вхідних параметрів шифру принаймні з одним параметром другого набору вхідних параметрів шифру. Додатково або альтернативно, схема керування дешифруванням 118 може бути зконфігурована для повторення процесу вибору найбільш вірогідної альтернативи для одного або більше вхідних параметрів шифру до тих пір, коли схема керування дешифруванням 118 зробить визначену кількість невдалих спроб вибрати найбільш вірогідну альтернативу для одного або більше вхідних значень шифру, у цій ситуації схема керування дешифруванням 118 може бути зконфігурована для ініціювання повторної синхронізації RLC як описано вище, щоб ініціалізувати принаймні один вхідний параметр шифру з передаючою апаратурою 104. Визначена кількість невдалих спроб автономної повторної синхронізації може, наприклад, бути повідомлена приймаючій апаратурі 102 через мережу передачі сигналів (наприклад, від передаючої апаратури 104), або схема керування дешифруванням 118 може бути попередньо зконфігурована для здійснення визначеної кількості невдалих спроб до ініціювання повторної синхронізації RLC.

[0048] У деяких варіантах втілення винаходу схема керування дешифруванням 118 не зконфігурована для ініціювання процедури повторної синхронізації шифрування у відповідь на кожне визначення, що відбулася помилка шифрування, а скоріше зконфігурована для ініціювання процедури повторної синхронізації шифрування після того, як відбулося визначена кількість послідовних помилок шифрування (наприклад, для визначеної кількості послідовно отриманих PDU). Визначена кількість може включати натуральне число більше нуля. Схема керування дешифруванням 118 може бути попередньо зконфігурована для визначеної кількості. В іншому прикладі схема керування дешифруванням 118 може бути зконфігурована для встановлення попередньо визначеного числа, базуючись принаймні частково на типі сервісу, з яким пов'язані PDU (наприклад, попередньо визначене число може рівнятися 3 для CS мовного сигналу по HSPA і 10 для потокового сервісу). Додатково або альтернативно, схема керування дешифруванням 118 може бути зконфігурована для встановлення попередньо визначеного числа, базуючись принаймні частково на отриманому повідомленні мережі передачі сигналів, переданому передаючою апаратурою 104. В цьому відношенні, схема керування шифруванням 126 може бути зконфігурована для встановлення визначеної кількості послідовних помилок шифрування, які схема керування дешифруванням 118 повинна виявити до ініціювання процедури повторної синхронізації шифрування. Тоді схема керування шифруванням 126 може генерувати повідомлення мережі передачі сигналів для передачі на приймаючу апаратуру 102 через комунікаційний інтерфейс 124, який визначає встановлене попередньо визначене число. У варіантах втілення винаходу, де схема керування дешифруванням 118 зконфігурована для ініціювання процедури повторної синхронізації шифрування, після того, як відбулось попередньо визначене число послідовних помилок шифрування, схема керування

дешифруванням 118 може бути зконфігурована для змінення показника лічильника, базуючись принаймні частково на кількості послідовних помилок шифрування, які відбулися при визначенні наявності помилки шифрування й ініціювання процедури повторної синхронізації шифрування, базуючись принаймні частково на попередньо визначеному взаємозв'язку між показником лічильника та попередньо визначеним числом. Наприклад, схема керування дешифруванням 118 може бути зконфігурована для збільшення або зменшення показника лічильника, коли схема керування дешифруванням 118 визначає виникнення помилки шифрування й ініціювання процедури повторної синхронізації шифрування, коли показник лічильника дорівнює граничним значенням, таким як, наприклад, попередньо визначеному числу (наприклад, якщо збільшується від початкового нульового показника лічильника) або нулю (наприклад, якщо зменшується від початкового попередньо визначеного числа показника лічильника). Однак, буде прийняте із вдячністю розуміння, що збільшення й зменшення показника лічильника забезпечене лише як приклади того, як схема керування дешифруванням 118 зконфігурована для коректування показника лічильника в деяких варіантах втілення винаходу. Крім того, типові початкові значення й граничні значення забезпечені лише як приклади, і схема керування дешифруванням 118 може бути зконфігурована для використання інших початкових значень та граничних значень.

[0049] У деяких варіантах втілення винаходу схема керування дешифруванням 118 зконфігурована для надання можливості виявлення помилок шифрування й перевірки виникнення помилки шифрування тільки коли виникає одна або більше умов. Наприклад, схема керування дешифруванням 118 може бути зконфігурована для надання можливості виявлення помилок шифрування тільки коли її зконфігуовано з використанням передаючої апаратури 104, так як через інформацію мережі передачі сигналів, переданою на приймаючу апаратуру 102 передаючою апаратурою 104. В цьому відношенні, схема керування шифруванням 126 може бути зконфігуована для надання можливості й/або ненадання можливості виявлення помилок шифрування схемою керування дешифруванням 118 шляхом ініціювання інформацією мережі передачі сигналів надання можливості й/або ненадання можливості виявлення помилок шифрування для передачі на приймаючу апаратуру 102 передаючою апаратурою 104. Інформація мережі передачі сигналів може додатково включати індикацію попередньо визначеного числа послідовних помилок шифрування, які відбулися, що схема керування дешифруванням 118 повинна виявити до ініціалізації процедури повторної синхронізації шифрування. Додатково або альтернативно, схема керування дешифруванням 118 може бути зконфігуована для надання можливості виявлення помилок шифрування, базуючись принаймні частково на типі сервісу, з яким пов'язаний отриманий PDU.

[0050] Фіг. 3 ілюструє блок-схему відповідно до типового методу виявлення помилки шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення винаходу. В цьому відношенні, Фіг. 3 ілюструє операції, які можуть бути виконані схемою керування дешифруванням 118. Метод може включати схему керування дешифруванням 118, що при операції 300 ініціалізує значення принаймні одного вхідного параметру шифру першого набору з одного або більше вхідних параметрів шифру з передаючою апаратурою 104. Операція 310 може включати схему керування дешифруванням 118, що використовує перший набір вхідних параметрів шифру для декодування зашифрованих даних в отриманому PDU. Тоді, при операції 320, схема керування дешифруванням 118 може порівнювати значення принаймні частини декодованих даних із очікуваним значенням. Операція 330 може включати схему керування дешифруванням 118, що визначає виникнення помилки шифрування коли значення принаймні частини декодованих даних не дорівнює очікуваним значенням. Тоді, при операції 340, схема керування дешифруванням 118 може ініціювати процедуру повторної синхронізації шифрування у відповідь на визначення (виникнення помилки).

[0051] Фіг. 4 ілюструє блок-схему відповідно до типового методу виявлення помилки шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення винаходу. В цьому відношенні, Фіг. 4 ілюструє операції, які можуть бути виконані схемою керування дешифруванням 118. Метод може включати схему керування дешифруванням 118, що при операції 400 ініціалізує значення принаймні одного вхідного параметру шифру першого набору з одного або більше вхідних параметрів шифру з передаючою апаратурою 104. Операція 410 може включати схему керування дешифруванням 118, що при операції 410 встановлює попередньо визначене число послідовних помилок шифрування, які повинні відбуватися до ініціалізації процедури повторної синхронізації шифрування. Схема керування дешифруванням 118 може зробити визначення операції 410, базуючись принаймні частково на інформації мережі передачі сигналів, переданої передаючою апаратурою 104 й/або типу сервісу, з яким пов'язаний отриманий PDU. Операція 420 може включати схему керування

дешифруванням 118, що встановлює виникнення попередньо визначеного числа послідовних помилок шифрування під час декодування послідовно одержаних PDU. Тоді, при операції 430, схема керування дешифруванням 118 може ініціювати процедуру повторної синхронізації шифрування у відповідь на визначення операції 420.

[0052] Фіг. 5 ілюструє блок-схему відповідно до типового методу виявлення помилки шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення винаходу. В цьому відношенні, Фіг. 5 ілюструє операції, які можуть бути виконані схемою керування шифруванням 126. Операція 500 може включати схему керування шифруванням 126, що ініціалізує значення принаймні одного вхідного параметру шифру другого набору з одного або більше вхідних параметрів шифру, які будуть використовуватися для того, щоб шифрувати дані, з приймаючою апаратурою 102. Тоді, при операції 510, схема керування шифруванням 126 може використовувати другий набір вхідних параметрів шифру для шифрування даних в PDU для передачі на приймаючу апаратуру 102. Операція 520 може опціонально включати схему керування шифруванням, що бере участь у процедурі повторної синхронізації шифрування з приймаючою апаратурою 102, коли приймаючою апаратурою виявлена помилка шифрування. Операція 520 може бути виконана у варіантах втілення винаходу, де схема керування дешифруванням 118 зконфігурована для ініціювання повторної синхронізації RLC.

[0053] Фіг. 6 ілюструє блок-схему відповідно до типового методу для виявлення помилки шифрування та відновлення безпомилкового стану відповідно до типового варіанту втілення винаходу. В цьому відношенні, Фіг. 6 ілюструє операції, які можуть бути виконані схемою керування шифруванням 126. Операція 600 може включати схему керування шифруванням 126, що ініціалізує значення принаймні одного вхідного параметру шифру другого набору з одного або більше вхідних параметрів шифру, які будуть використовуватися для того, щоб шифрувати дані, з приймаючою апаратурою 102. Тоді схема керування шифруванням 126 може викликати передачу повідомлення мережі передачі сигналів, що конфігурує виявлення помилок шифрування, на приймаючу апаратуру 102. Повідомлення мережі передачі сигналів може включати команди, що роблять можливим виявлення помилок шифрування приймаючою апаратурою 102, команди, що встановлюють попередньо визначене число послідовних помилок шифрування, що відбулися, які приймаюча апаратура 102 повинна визначити до ініціювання процедури повторної синхронізації шифрування, й/або попередньо визначену кількість невдалих спроб автономної повторної синхронізації, яку приймаюча апаратура 102 повинна зробити до ініціалізації процедури повторної синхронізації RLC. Тоді, при операції 620, схема керування шифруванням 126 може використовувати другий набір вхідних параметрів шифру, щоб шифрувати дані в PDU для передачі на приймаючу апаратуру 102. Операція 630 може опціонально включати схему керування шифруванням, що бере участь у процедурі повторної синхронізації шифрування з приймаючою апаратурою 102, коли приймаючою апаратурою виявлена помилка шифрування (наприклад, попередньо визначене число послідовних помилок шифрування). Операція 630 може бути виконана у варіантах втілення винаходу, де схема керування дешифруванням 118 зконфігурована для ініціювання повторної синхронізації RLC.

[0054] РИСУНКИ 3-6 є блок-схемами системи, методу та комп'ютерного програмного продукту відповідно до типового варіанту втілення винаходу. Мається на увазі, що кожний блок або крок блок-схем, та комбінації блоків у блок-схемах, можуть бути здійснені різними засобами, такими як апаратні засоби й/або комп'ютерний програмний продукт, що включає один або більше комп'ютерно-зчитуємих засобів, які мають комп'ютерно-зчитуємі програмні команди, що зберігаються на них. Наприклад, одна або більше процедур, описаних у цьому документі, можуть бути реалізовані комп'ютерними програмними командами комп'ютерного програмного продукту. В цьому відношенні, комп'ютерні програмні продукт(и), які містять у собі процедури, описані у цьому документі, можуть зберігатися одним або більше запам'ятовуваними пристроями приймаючої апаратури 102, передаючої апаратури 104, мобільного терміналу, серверу, або іншого обчислювального пристрою та виконуватись процесором в обчислювальному пристрої (наприклад, процесором 110 й/або процесором 120). У деяких варіантах втілення винаходу комп'ютерні програмні команди, які включають комп'ютерні програмні продукт(и), які містять у собі описані вище процедури, можуть бути збережені запам'ятовуваними пристроями багатьох обчислювальних пристроїв. Буде прийняте із вдячністю розуміння, що будь-який такий комп'ютерний програмний продукт може бути завантажений на комп'ютер або іншу апаратуру, що програмується, щоб зробити пристрій, таким чином комп'ютерний програмний продукт, що включає команди, які виконуються на комп'ютері або іншій апаратурі, що програмується, створює засоби реалізації функцій, визначених в блоці(ах) блок-схеми або кроці(ах). Крім того, комп'ютерний програмний продукт може включати один або більше блоків запам'ятовуваних пристроїв, що зчитуються комп'ютером, у яких команди



комп'ютерної програми можуть бути збережені таким чином, щоб один або більше блоків запам'ятовуючих пристроїв, що зчитуються комп'ютером, могли керувати комп'ютером або іншою апаратурою, що програмується, для функціонування специфічним способом, таким чином комп'ютерний програмний продукт включає виріб, що здійснює функції, перелічені в блоці(ах) блок-схеми або кроці(ах). Команди комп'ютерної програми одного або більше комп'ютерних програмних продуктів можуть також бути завантажені на комп'ютер або іншу апаратуру, що програмується, щоб викликати серію операційних кроків, які будуть виконані на комп'ютері або іншій апаратурі, що програмується, щоб зробити комп'ютерно-здійснювальний процес таким чином, щоб команди, які виконуються на комп'ютері або іншій апаратурі, що програмується, забезпечили кроки для реалізації функцій, визначених в блоці(ах) блок-схеми або кроці(ах).

[0055] Відповідно, блоки або кроки блок-схеми забезпечують комбінації засобів для виконання зазначених функцій й комбінації кроків для виконання зазначених функцій. Також мається на увазі, що один або більше блоків або кроки блок-схеми, та комбінації блоків або кроків у блок-схемі, можуть бути здійснені апаратними комп'ютерними системами особливого призначення, які виконують чітко визначені функції або кроки, або комбінацією апаратних засобів особливого призначення та комп'ютерного програмного продукту(ів).

[0056] Вищеописані функції можуть бути виконані різними способами. Наприклад, можуть використовуватися будь-які підходящі засоби для того, щоб виконувати кожну з вищеописаних функцій, щоб забезпечити варіанти втілення винаходу. В одному варіанті втілення винаходу відповідно зконфігурований процесор може забезпечити всі або частину елементів винаходу. В іншому варіанті втілення винаходу всі або частина елементів винаходу можуть бути зконфігуровані й працювати під керуванням комп'ютерного програмного продукту. Комп'ютерний програмний продукт для виконання методу варіантів втілення винаходу включає комп'ютерно-зчитуємий носій інформації, такий як енергонезалежний носій інформації, та частини коду програми, що зчитуються комп'ютером, такі як серія комп'ютерних команд, які містять у собі комп'ютерно-зчитуємий носій інформації.

[0057] Тоді, по суті, деякі варіанти втілення винаходу забезпечують кілька переваг для обчислювальних пристроїв, користувачів обчислювальних пристроїв та мережевих операторів. Варіанти втілення винаходу забезпечують приймаючу апаратуру, зконфігуровану для визначення виникнення помилки шифрування. В цьому відношенні, варіанти втілення винаходу забезпечують приймаючу апаратуру, зконфігуровану для визначення виникнення помилки шифрування, порівнюючи значення декодованих даних із очікуваним значенням, щоб визначити, чи дорівнює значення декодованих даних очікуваним значенням. Це порівняння дозволяє деяким варіантам втілення винаходу визначати виникнення помилки шифрування незалежно від типу сервісу, з яким пов'язаний зашифрований модуль протоколу даних. Варіанти втілення винаходу забезпечують приймаючу апаратуру 102, зконфігуровану для визначення виникнення помилки шифрування в ситуаціях, де контроль циклічним надлишковим кодом (CRC) для CRC захищених даних може зазнавати невдачі.

[0058] Крім того, варіанти втілення винаходу забезпечують приймаючу апаратуру, зконфігуровану для ініціювання процедури виправлення помилок шифрування, щоб повторно синхронізувати локальний набір з одного або більше вхідних параметрів шифру, що використовувались для декодування отриманих зашифрованих даних, з набором з одного або більше вхідних параметрів шифру, використаних передаючою апаратурою, щоб шифрувати зашифровані дані до передачі на термінал. Деякі варіанти втілення винаходу забезпечують приймаючу апаратуру, зконфігуровану для ініціювання керованої по радіоканалу повторної синхронізації з передаючою апаратурою, щоб повторно синхронізувати один або більше вхідних параметрів шифру. Варіанти втілення винаходу також забезпечують приймаючу апаратуру, зконфігуровану для автономної повторної синхронізації одного або більше вхідних параметрів шифру шляхом вибору найбільш вірогідного альтернативного значення принаймні для одного вхідного параметру шифру. Варіанти втілення винаходу забезпечують для мережі із передачею сигналів конфігурації процедур виявлення помилок шифрування для й/або виправлення помилок шифрування, що усувають проблеми функціональної сумісності, які можуть відбутися, коли приймаюча апаратура, зконфігурована для визначення виникнення помилки шифрування й/або ініціювання процедури виправлення помилок шифрування, взаємодіє по мережі, не зконфігурованій, щоб забезпечити процедуру виправлення помилок шифрування.

[0059] Багато модифікацій і інші варіанти втілення винаходу, сформульованого у цьому документі, придуть на розум тому, хто кваліфікований у галузі техніки, до якої ці винаходи належать, маючи перевагу від вивчення представленого в попередніх описах та пов'язаних рисунках. Тому, потрібно мати на увазі, що варіанти втілення винаходу не повинні бути

обмежені певними розкритими варіантами втілення винаходу й що модифікації й інші варіанти втілення призначені, щоб бути включеними в обсяг прикладеної формули винаходу.

Крім того, незважаючи на те, що попередні описи й пов'язані рисунки описують типові варіанти втілення винаходу в контексті певних типових комбінацій елементів й/або функцій, потрібно прийняти до уваги, що різні комбінації елементів й/або функцій можуть бути забезпечені альтернативними варіантами втілення винаходу, не відступаючи від обсягу прикладеної формули винаходу. В цьому відношенні, наприклад, різні комбінації елементів й/або функцій ніж ті, що детально описані вище, також розглянуті, що може бути сформульовано у деяких із пунктів прикладеної формули винаходу. Незважаючи на те, що в цьому документі використовуються певні спеціальні терміни, вони використовуються лише в універсальному й описовому розумінні, а не з метою обмеження.

## ФОРМУЛА ВИНАХОДУ

1. Спосіб виявлення помилок шифрування й відновлення безпомилкового стану, який включає: використання першого набору з одного або більше вхідних параметрів шифру для декодування зашифрованих даних в отриманому модулі даних протоколу, де зашифровані дані були закодовані, використовуючи другий набір з одного або більше вхідних параметрів шифру; порівняння значення принаймні частини декодованих даних із очікуваним значенням; визначення, із схемою керування дешифруванням, виникнення помилки шифрування, коли значення принаймні частини декодованих даних не дорівнює очікуваному значенню; та ініціювання процедури повторної синхронізації шифрування у відповідь на визначення, що відбулася помилка шифрування, щоб повторно синхронізувати принаймні один з першого набору вхідних параметрів шифру принаймні з одним із другого набору вхідних параметрів шифру.

2. Спосіб за п. 1, який додатково включає: коректування показника лічильника, базуючись принаймні частково на кількості послідовних помилок шифрування, які відбулися при декодуванні зашифрованих даних в отриманих модулях даних протоколу; та де ініціювання процедури повторної синхронізації шифрування включає ініціювання процедури повторної синхронізації шифрування, коли показник лічильника має попередньо визначені взаємозв'язки з попередньо визначеним числом, де попередньо визначене число включає натуральне число більше нуля.

3. Спосіб за п. 2, який додатково включає встановлення попередньо визначеного числа, базуючись принаймні частково на одному або більше повідомленнях, переданих передавальною апаратурою, або типі сервісу, з яким пов'язані модулі даних протоколу.

4. Спосіб за п. 1, за яким ініціювання процедури повторної синхронізації шифрування включає ініціювання процедури керування по радіоканалу повторної синхронізації для ініціалізації принаймні одного вхідного параметра шифру таким чином, щоб перший набір вхідних параметрів шифру був повторно синхронізований із другим набором вхідних параметрів шифру.

5. Спосіб за п. 1, за яким ініціювання процедури повторної синхронізації шифрування включає ініціювання автономної процедури повторної синхронізації шифрування, що включає: вибір найбільш вірогідного альтернативного значення для принаймні одного з першого набору вхідних параметрів шифру; та використання вибраного найбільш вірогідного альтернативного значення для декодування зашифрованих даних в отриманому модулі даних протоколу.

6. Спосіб за п. 1, за яким принаймні частина декодованих даних включає одне або більше додаткове поле, індикатор довжини або заголовок модуля даних протоколу.

7. Спосіб за п. 1, за яким модуль даних протоколу включає модуль даних протоколу непідтвердженого режиму рівня керування радіоканалу, модуль даних протоколу підтвердженого режиму рівня керування радіоканалу, модуль даних протоколу непідтвердженого режиму протоколу конвергенції пакетної передачі даних або модуль даних протоколу підтвердженого режиму протоколу конвергенції пакетної передачі даних.

8. Пристрій для виявлення помилок шифрування та відновлення безпомилкового стану, який містить принаймні один процесор і принаймні один запам'ятовуючий пристрій, що зберігає комп'ютерний програмний код, де принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код, сконфігуровані принаймні з одним процесором, змушують апаратуру до принаймні: використання першого набору з одного або більше вхідних параметрів шифру для декодування зашифрованих даних в отриманому модулі даних протоколу, де зашифровані дані

були закодовані із використанням другого набору з одного або більше вхідних параметрів шифру;

порівнювання значення принаймні частини декодованих даних з очікуваним значенням;

визначення виникнення помилки шифрування, коли значення принаймні частини декодованих даних не дорівнює очікуваному значенню; та

ініціювання процедури повторної синхронізації шифрування у відповідь на визначення, що відбулася помилка шифрування, щоб повторно синхронізувати принаймні один з першого набору вхідних параметрів шифру із принаймні одним із другого набору вхідних параметрів шифру.

9. Пристрій за п. 8, в якому принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код, сконфігуровані принаймні з одним процесором, додатково змушують апаратуру:

коректувати показник лічильника, базуючись принаймні частково на кількості послідовних помилок шифрування, які відбулися при декодуванні зашифрованих даних в отриманих модулях даних протоколу; та де

принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код сконфігуровані принаймні з одним процесором, змушують апаратуру ініціювати процедуру повторної синхронізації шифрування шляхом ініціювання процедури повторної синхронізації шифрування, коли показник лічильника має попередньо визначений взаємозв'язок з попередньо визначеним числом, де попередньо визначене число містить натуральне число більше нуля.

10. Пристрій за п. 9, в якому принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код, сконфігуровані принаймні з одним процесором, додатково змушують апаратуру встановлювати попередньо визначене число, базуючись принаймні частково на одному або більше повідомленнях, переданих передавальною апаратурою або на типі сервісу, з яким пов'язані модулі даних протоколу.

11. Пристрій за п. 8, в якому принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код, сконфігуровані принаймні з одним процесором, змушують апаратуру ініціювати процедуру повторної синхронізації шифрування шляхом ініціювання керованої по радіоканалу процедури повторної синхронізації для ініціалізації принаймні одного вхідного параметра шифру таким чином, щоб перший набір вхідних параметрів шифру був повторно синхронізований із другим набором вхідних параметрів шифру.

12. Пристрій за п. 8, в якому принаймні один запам'ятовуючий пристрій та збережений комп'ютерний програмний код, сконфігуровані принаймні з одним процесором, змушують апаратуру ініціювати процедуру повторної синхронізації шифрування шляхом ініціювання автономної процедури повторної синхронізації шифрування, де автономна процедура повторної синхронізації шифрування включає:

вибір найбільш вірогідного альтернативного значення для принаймні одного з першого набору вхідних параметрів шифру; та

використання вибраного найбільш вірогідного альтернативного значення для декодування зашифрованих даних в отриманому модулі даних протоколу.

13. Пристрій за п. 8, в якому принаймні частина декодованих даних включає одне або більше додаткове поле, індикатор довжини або заголовок модуля даних протоколу.

14. Пристрій за п. 8, в якому модуль даних протоколу включає модуль даних протоколу непідтвердженого режиму рівня керування радіоканалу, модуль даних протоколу підтвердженого режиму рівня керування радіоканалу, модуль даних протоколу непідтвердженого режиму протоколу конвергенції пакетної передачі даних або модуль даних протоколу підтвердженого режиму протоколу конвергенції пакетної передачі даних.

15. Пристрій за п. 8, в якому пристрій містить або є реалізованим на мобільному телефоні, мобільний телефон включає схему інтерфейсу користувача й програмне забезпечення інтерфейсу користувача, збережене на одному або більше з принаймні одного запам'ятовуючого пристрою; де схема інтерфейсу користувача й програмне забезпечення інтерфейсу користувача сконфігуровані для того, щоб:

полегшити користувачу управління принаймні деякими функціями мобільного телефону завдяки використанню дисплея; та

змусити принаймні частину інтерфейсу користувача мобільного телефону відображатися на дисплеї, щоб полегшити користувачу управління принаймні деякими функціями мобільного телефону.

16. Комп'ютерно-зчитуваний носій інформації, що зберігає комп'ютерно-зчитувані програмні команди, комп'ютерно-зчитувані програмні команди сконфігуровані для виконання способу відповідно до будь-якого з пп. 1-6 під час виконання процесором.

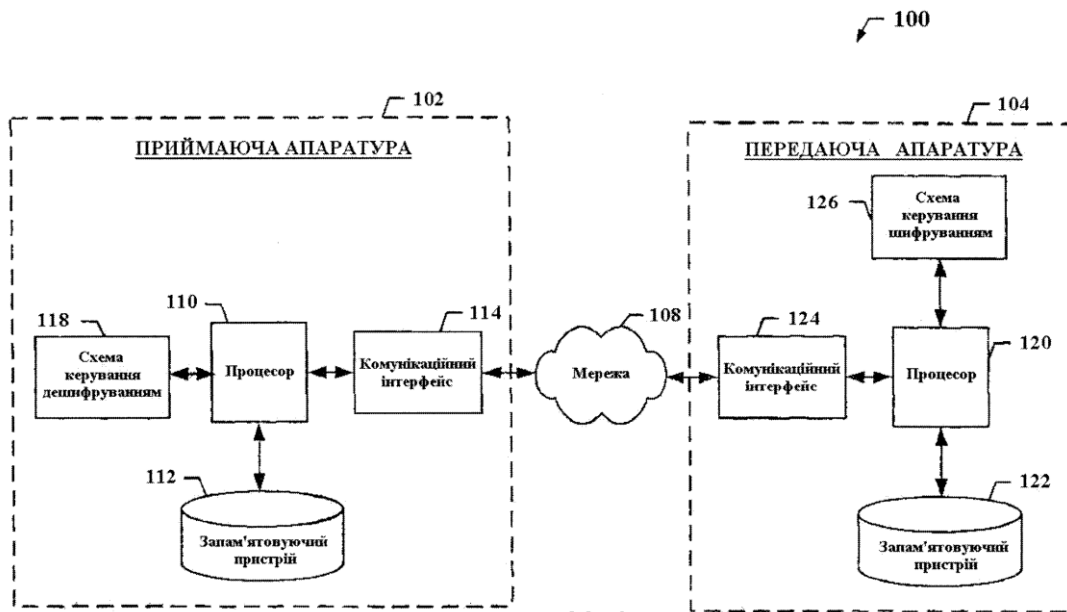


Fig. 1

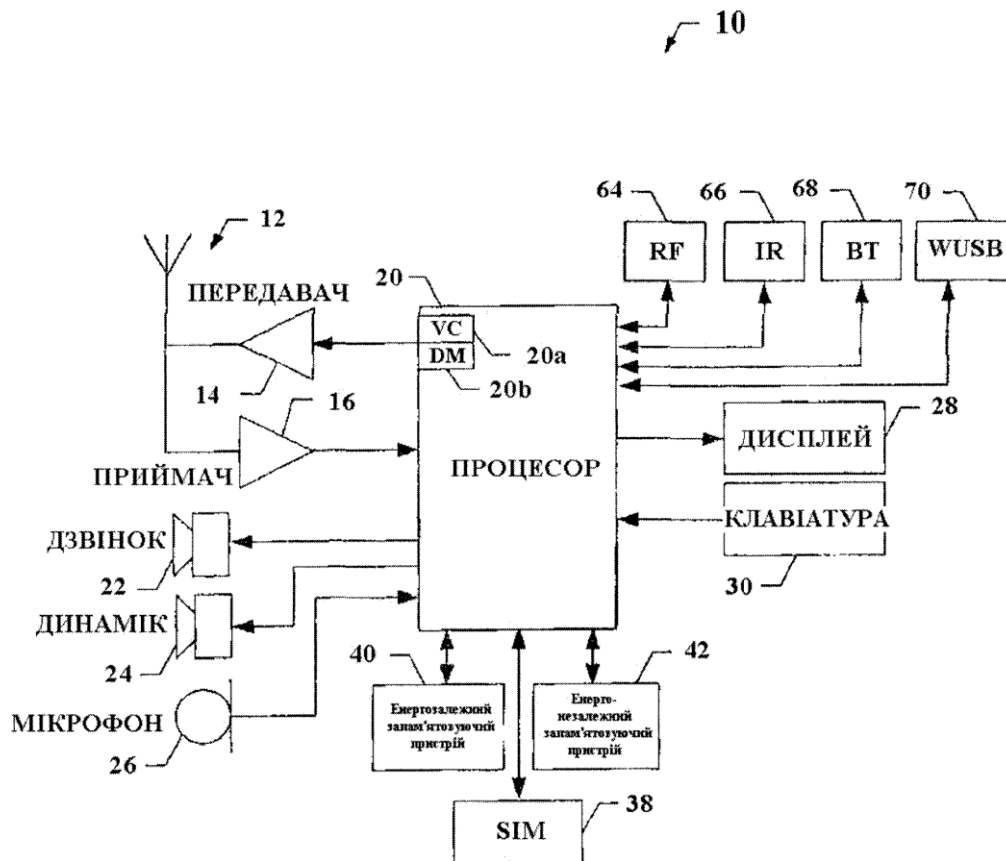


Fig. 2



Fig. 3

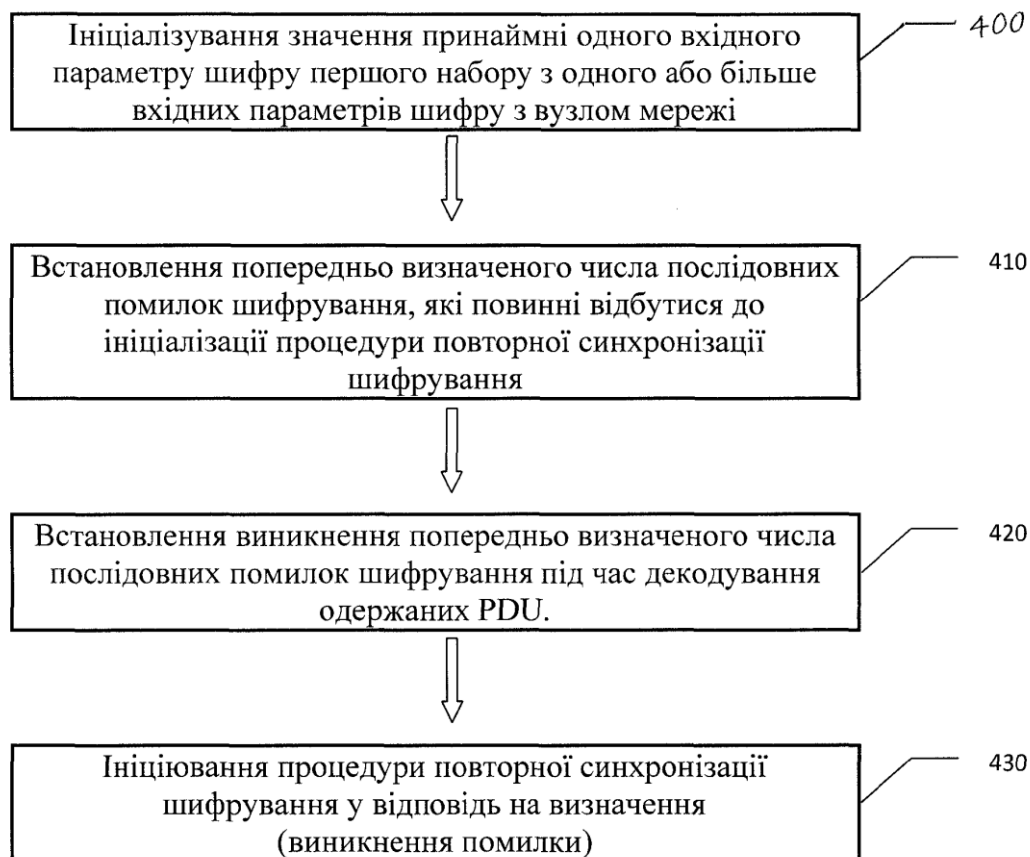


Fig. 4

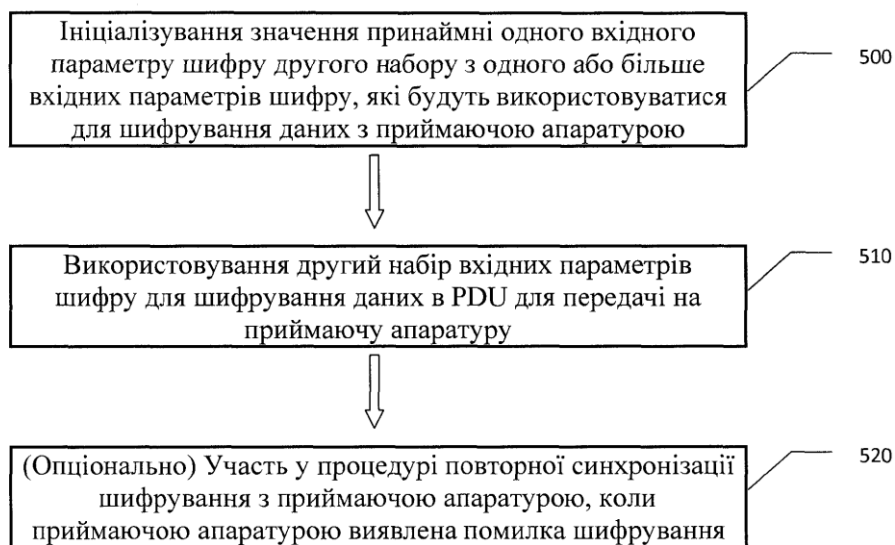


Fig. 5



Фіг. 6