



УКРАЇНА

(19) **UA** (11) **106531** (13) **C2**
(51) МПК (2014.01)
H04W 36/00
H04W 12/04 (2009.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

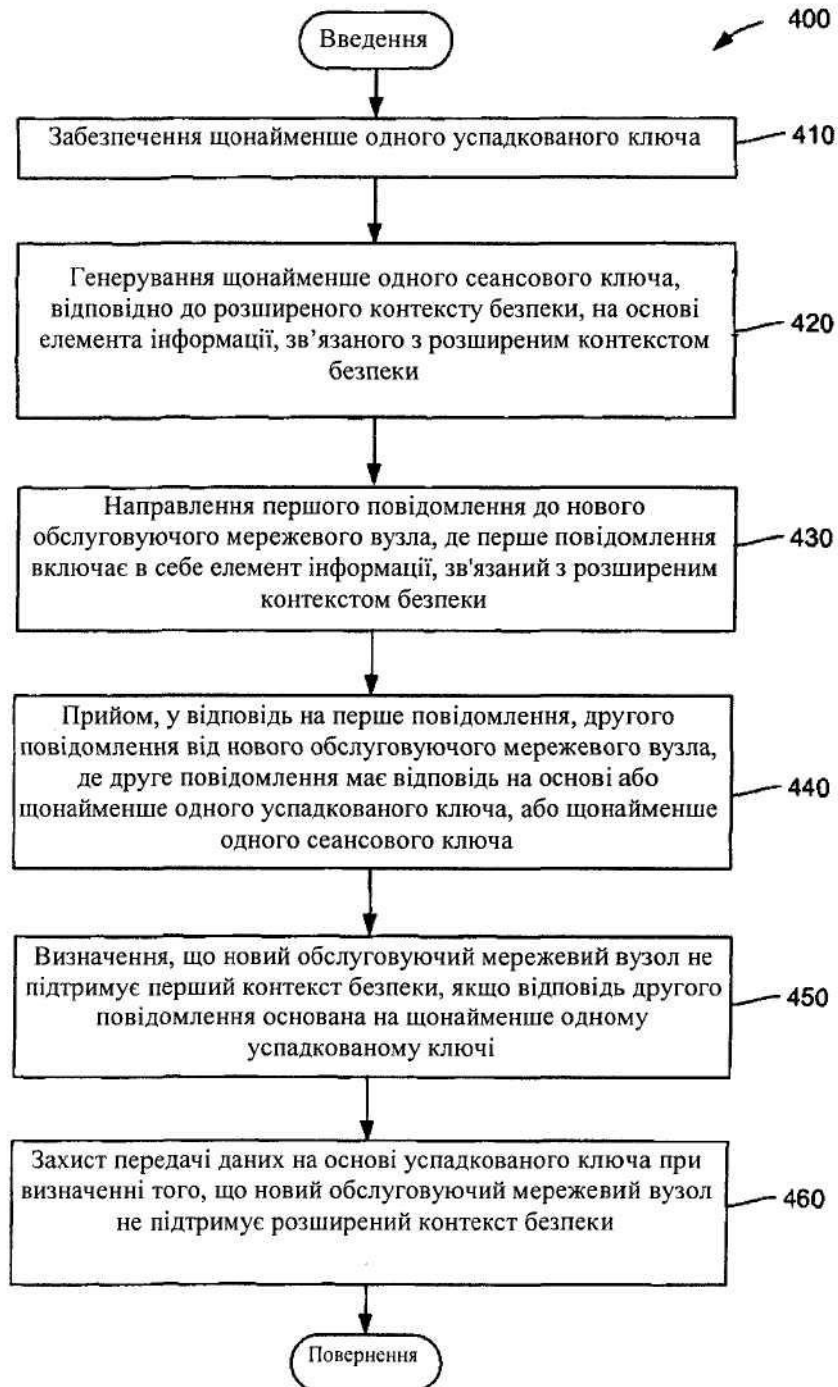
(21) Номер заявки:	а 2012 13040	(72) Винахідник(и):	Ескотт Едріан Едвард (US), Паланігоундер Ананд (US)
(22) Дата подання заявки:	15.04.2011	(73) Власник(и):	КВЕЛКОММ ІНКОРПОРЕЙТЕД, 5775 Morehouse Drive, San Diego, California 92121-1714, United States of America (US)
(24) Дата, з якої є чинними права на винахід:	10.09.2014	(74) Представник:	Мошинська Ніна Миколаївна, реєстр. №115
(31) Номер попередньої заявки відповідно до Паризької конвенції:	61/324,991, 13/084,353	(56) Перелік документів, взятих до уваги експертизою:	WO 2008092999 A1, 07.08.2008 WO 2009020789 A2, 12.02.2009 WO 2009/008627 A2, 15.01.2009 EP 2139260 A1, 30.01.2009 ETSI TS 133 102 V8.1.0 (2009-01) . Technical Specification Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102 version 8.1.0 Release 8) 3GPP TS 33.401 V8.1.1 (2008-10). Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture
(32) Дата подання попередньої заявки відповідно до Паризької конвенції:	16.04.2010, 11.04.2011		
(33) Код держави-учасниці Паризької конвенції, до якої подано попередню заявку:	US, US		
(41) Публікація відомостей про заявку:	25.02.2013, Бюл.№ 4		
(46) Публікація відомостей про видачу патенту:	10.09.2014, Бюл.№ 17		
(86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ	PCT/US2011/032754, 15.04.2011		

(54) ПРИСТРІЙ І СПОСІБ ПЕРЕХОДУ ВІД ОБСЛУГОВУЮЧОГО МЕРЕЖЕВОГО ВУЗЛА, ЯКИЙ ПІДТРИМУЄ РОЗШИРЕНИЙ КОНТЕКСТ БЕЗПЕКИ, ДО УСПАДКОВАНОГО ОБСЛУГОВУЮЧОГО МЕРЕЖЕВОГО ВУЗЛА

(57) Реферат:

Розкритий спосіб переходу віддаленого терміналу від поточного обслуговуючого мережевого вузла, що має розширений контекст безпеки, до нового обслуговуючого мережевого вузла. У способі, віддалений термінал забезпечує щонайменше один успадкований ключ і генерує щонайменше один сеансовий ключ на основі елемента інформації, зв'язаного з розширеним контекстом безпеки. Віддалений термінал направляє перше повідомлення, що має елемент інформації, до нового обслуговуючого мережевого вузла. Віддалений термінал приймає друге повідомлення, від нового обслуговуючого мережевого вузла, що має відповідь на основі або успадкованого ключа, або сеансового ключа. Віддалений термінал визначає, що новий обслуговуючий мережевий вузол не підтримує розширений контекст безпеки, якщо відповідь другого повідомлення ґрунтується на успадкованому ключі. Відповідно, віддалений термінал захищає передачу даних, ґрунтуючись на успадкованому ключі, при визначенні, що розширений контекст безпеки не підтримується.

UA 106531 C2



Фіг. 4

ПЕРЕХРЕСНЕ ПОСИЛАННЯ НА СПОРІДНЕНІ ЗАЯВКИ

Дана заявка заявляє пріоритет попередньої заявки США №61/324991, поданої 16 квітня 2010 року, яка включена сюди за допомогою посилання.

ГАЛУЗЬ ТЕХНІКИ, ДО ЯКОЇ НАЛЕЖИТЬ ВІНАХІД

5 Даний винахід стосується загалом розширеного контексту безпеки для користувацького обладнання, яке працює в універсальній системі мобільного зв'язку (UMTS), GSM бездротової мережі радіодоступу (GERAN), і/або лінійному обладнанні системи передачі (LTE) або виділеній наземній мережі радіодоступу UMTS (E-UTRAN).

РІВЕНЬ ТЕХНІКИ

10 Успішна аутентифікація АКА (Аутентифікація і узгодження ключа) в мережі LTE четвертого покоління (4G) або (в мережі радіодоступу UMTS третього покоління (3G) або в мережах GERAN, що використовують 3G АКА аутентифікацію приводить до пари спільно використовуваних ключів, ключа (СК) до шифру і ключа (ІК) цілісності для забезпечення захисту передач даних між користувацьким обладнанням (UE) і мережею. Спільно використовувані
15 ключі можуть бути використані безпосередньо для забезпечення захисту трафіка між UE і мережею, як у випадку UTRAN (наземної мережі радіодоступу UMTS), або можуть бути використані для статичного отримання ключів, наприклад, KASME або ключів, отриманих від неї, у випадку E-UTRAN і Kc або Kc128, у випадку GERAN (GSM Edge бездротової мережі радіодоступу).

20 Компрометований ключ може привести до серйозних проблем безпеки доти, поки ключі не замінюються на наступній аутентифікації АКА. Як правило, аутентифікація АКА не виконується часто через значні необхідні витрати. Крім того, якщо обидва ключі (СК і ІК) компрометовані, то ключі, що використовуються між UE і обслуговуючою мережею радіодоступу можуть також стати компрометованими.

25 У застосуваннях UMTS/HSPA (високошвидкісний пакетний доступ), всі або деякі з функціональних можливостей контролера радіомережі (RNC) і вузла В можуть бути стягнуті разом в один вузол на границі цієї мережі. RNC потребує ключів для функціональних можливостей, таких як шифрування площини користувача і сигналізація шифрування площини користувача і захист цілісності. Проте, функціональна можливість RNC може бути розгорнена в
30 незахищеному місцеположенні, такому як, у власному вузлі В в фемтостільнику UMTS. Відповідно, функціональні можливості RNC, розгорнені в можливо небезпечних місцеположеннях, що забезпечують доступ (включаючи в себе фізичний доступ) можуть дозволити ключам СК і ІК бути компрометованими.

35 Сеансові ключі (змінена версія СК і ІК) можуть бути використані, щоб знижувати ризики безпеки, пов'язані з незахищеною функціональною можливістю RNC. Способи для забезпечення таких сеансових ключів розкриваються в Публікації Заявки на патент США № US 2007/0230707 A1.

На жаль, використання таких сеансових ключів вимагає змін модернізації для обслуговуючої мережі. Проте, оператори мереж можуть модернізувати обслуговуючі мережі поетапно.

40 Тому існує необхідність в методиці для віддаленого терміналу для взаємодії з обслуговуючими мережевими вузлами, які підтримують розширений контекст безпеки і з успадкованими обслуговуючими мережевими вузлами.

СУТЬ ВІНАХОДУ

45 Аспект даного винаходу може полягати в способі переходу віддаленого терміналу від поточного обслуговуючого мережевого вузла, що має перший контекст безпеки до нового обслуговуючого мережевого вузла. У способі, віддалений термінал забезпечує щонайменше один успадкований ключ, зв'язаний з другим контекстом безпеки, причому перший контекст безпеки включає в себе властивість безпеки, яка не підтримується другим контекстом безпеки. Віддалений термінал генерує щонайменше один сеансовий ключ, відповідно до першого
50 контексту безпеки, на основі елемента інформації, зв'язаного з першим контекстом безпеки. Віддалений термінал направляє перше повідомлення до нового обслуговуючого мережевого вузла. Перше повідомлення включає в себе елемент інформації, зв'язаний з першим контекстом безпеки. Віддалений термінал приймає у відповідь на перше повідомлення друге повідомлення від нового обслуговуючого мережевого вузла. Друге повідомлення має відповідь
55 на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа. Віддалений термінал визначає, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення оснований на щонайменше одному успадкованому ключі. Відповідно, віддалений термінал захищає передачі даних на основі щонайменше одного успадкованого ключа при визначенні того, що новий обслуговуючий
60 мережевий вузол не підтримує перший контекст безпеки.

У більш докладних аспектах винаходу, елемент інформації може містити значення відліку. Значення відліку може оновлюватися за сеанс. Перший контекст безпеки може бути розширеним контекстом безпеки UMTS, і другий контекст безпеки є успадкованим контекстом безпеки. Друге повідомлення може включати в себе код аутентифікації повідомлення (MAC) і віддалений термінал може визначати, що відповідь оснований на щонайменше одному успадкованому ключі, за допомогою визначення, що MAC був обчислений з використанням щонайменше одного успадкованого ключа. Віддалений термінал може містити мобільне користувацьке обладнання.

Інший аспект винаходу може полягати у віддаленому терміналі, який може включати в себе засіб для забезпечення щонайменше одного успадкованого ключа, зв'язаного з другим контекстом безпеки, причому перший контекст безпеки поточного обслуговуючого мережевого вузла включає в себе властивість безпеки, яка не підтримується другим контекстом безпеки; засіб для генерування щонайменше одного сеансового ключа, відповідно до першого контексту безпеки, на основі елемента інформації, зв'язаного з першим контекстом безпеки; засіб для направлення першого повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе сигналізацію елемента інформації, зв'язану з першим контекстом безпеки; засіб для прийому, у відповідь на перше повідомлення, другого повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа; засіб для визначення того, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення оснований на щонайменше одному успадкованому ключі і засіб для захисту передач даних на основі щонайменше одного успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки.

Інший аспект винаходу може полягати у віддаленому терміналі, який може включати в себе процесор, сконфігурований з можливістю: забезпечення щонайменше одного успадкованого ключа, зв'язаного з другим контекстом безпеки, причому перший контекст безпеки поточного обслуговуючого мережевого вузла включає в себе властивість безпеки, яка не підтримується другим контекстом безпеки; генерування щонайменше одного сеансового ключа, відповідно до першого контексту безпеки, на основі елемента інформації, зв'язаного з першим контекстом безпеки; направлення першого повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе елемент інформації, зв'язаний з першим контекстом безпеки; прийому, у відповідь на перше повідомлення, другого повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа; визначення, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення оснований на щонайменше одному успадкованому ключі; і захисту передач даних на основі щонайменше одного успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки.

Інший аспект винаходу може полягати в комп'ютерному програмному продукті, що містить машиночитаний носій зберігання, що містить код для спонукання комп'ютера забезпечувати щонайменше один успадкований ключ, зв'язаний з другим контекстом безпеки, причому перший контекст безпеки поточного обслуговуючого мережевого вузла включає в себе властивість безпеки, яка не підтримується другим контекстом безпеки; код для спонукання комп'ютера генерувати щонайменше один сеансовий ключ, відповідно до першого контексту безпеки, на основі елемента інформації, зв'язаного з першим контекстом безпеки; код для спонукання комп'ютера направляти перше повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе елемент інформації, зв'язаний з першим контекстом безпеки; код для спонукання комп'ютера приймати, у відповідь на перше повідомлення, другого повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа; код для спонукання комп'ютера визначати, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення оснований на щонайменше одному успадкованому ключі; і код для спонукання комп'ютера захищати передачі даних на основі щонайменше одного успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки.

КОРОТКИЙ ОПИС КРЕСЛЕНЬ

Фіг. 1 є блок-схемою зразкової системи бездротового зв'язку.

Фіг. 2 є блок-схемою зразкової системи бездротового зв'язку відповідно до архітектури UMTS/UTRAN.

Фіг. 3 є блок-схемою зразкової системи бездротового зв'язку відповідно до архітектури GERAN.

5 Фіг. 4 є блок-схемою послідовності операцій способу переходу віддаленого терміналу від обслуговуючого мережевого вузла, що має розширений контекст безпеки до нового обслуговуючого мережевого вузла.

Фіг. 5 є блок-схемою послідовності операцій способу встановлення розширеного контексту безпеки між віддаленим терміналом і обслуговуючою мережею на основі повідомлення запиту прикріплення.

10 Фіг. 6 є блок-схемою послідовності операцій способу встановлення щонайменше одного сеансового ключа від розширеного контексту безпеки між віддаленим терміналом і обслуговуючою мережею на основі повідомлення запиту обслуговування.

15 Фіг. 7 є блок-схемою послідовності операцій способу встановлення щонайменше одного сеансового ключа від розширеного контексту безпеки між віддаленим терміналом і обслуговуючою мережею на основі повідомлення запиту оновлення області трасування.

Фіг. 8 є блок-схемою комп'ютера, що включає в себе процесор і пам'ять.

Фіг. 9 є блок-схемою зразкової системи бездротового зв'язку відповідно до архітектури E-UTRAN.

20 Фіг. 10 є блок-схемою послідовності операцій способу переходу віддаленого терміналу від обслуговуючого мережевого вузла, що має розширений контекст безпеки до нового обслуговуючого мережевого вузла.

ДОКЛАДНИЙ ОПИС

25 Слово "зразковий" використовується тут для позначення "служить як приклад, зразок або ілюстрація". Будь-який варіант втілення, описаний тут як "зразковий", не обов'язково повинен розглядатися як переважний або переважний в порівнянні з іншими варіантами втілень.

Посилаючись на Фіг. 2-4, аспект даного винаходу може полягати в способі 400 переходу віддаленого терміналу 210 від обслуговуючого мережевого вузла 230, що має розширений контекст безпеки до нового обслуговуючого мережевого вузла 230'. У способі, віддалений термінал забезпечує щонайменше один успадкований ключ (етап 410) і генерує щонайменше один сеансовий ключ, відповідно до розширеного контексту безпеки, на основі елемента інформації, зв'язаного з розширеним контекстом безпеки (етап 420). Віддалений термінал направляє перше повідомлення до нового обслуговуючого мережевого вузла (етап 430). Перше повідомлення включає в себе елемент інформації, зв'язаний з розширеним контекстом безпеки. 35 Віддалений термінал приймає, у відповідь на перше повідомлення, друге повідомлення від нового обслуговуючого мережевого вузла (етап 440). Друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа. Віддалений термінал визначає, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення оснований на щонайменше одному успадкованому ключі (етап 450). Відповідно, віддалений термінал захищає передачу даних на основі успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує розширений контекст безпеки (етап 460). Елемент інформації може містити значення відліку.

Посилаючись додатково на Фіг. 8, інший аспект винаходу може полягати у віддаленому терміналі 210, який може включати в себе засіб (процесор 810) для забезпечення щонайменше одного успадкованого ключа; засіб для генерування щонайменше одного сеансового ключа відповідно до розширеного контексту безпеки, на основі елемента інформації, зв'язаного з розширеним контекстом безпеки; засіб для направлення першого повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе сигналізацію елемента інформації відповідно до розширеного контексту безпеки; засіб для прийому, у 50 відповідь на перше повідомлення, другого повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа; засіб для визначення того, що новий обслуговуючий мережевий вузол не підтримує розширений контекст безпеки, якщо 55 відповідь другого повідомлення оснований на успадкованому ключі; і засіб для захисту передачі даних на основі успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує розширений контекст безпеки.

Інший аспект винаходу може полягати у віддаленому терміналі 210, який може включати в себе процесор 810, сконфігурований з можливістю: забезпечення щонайменше одного 60 успадкованого ключа; генерування щонайменше одного сеансового ключа, відповідно до

розширеного контексту безпеки, на основі елемента інформації, зв'язаного з розширеним контекстом безпеки; направлення першого повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе елемент інформації, зв'язаний з розширеним контекстом безпеки; прийому, у відповідь на перше повідомлення, другого повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа; визначення того, що новий обслуговуючий мережевий вузол не підтримує розширений контекст безпеки, якщо відповідь другого повідомлення оснований на успадкованому ключі; і засіб для захисту передачі даних на основі успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує розширений контекст безпеки.

Інший аспект винаходу може полягати в комп'ютерному програмному продукті, що містить машиночитаний носій 820 зберігання, що містить код для спонукання комп'ютера 800 забезпечувати щонайменше один успадкований ключ; код для спонукання комп'ютера генерувати щонайменше один сеансовий ключ, відповідно до розширеного контексту безпеки, на основі елемента інформації, зв'язаного з розширеним контекстом безпеки; код для спонукання комп'ютера направляти перше повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе елемент інформації, зв'язаний з розширеним контекстом безпеки; код для спонукання комп'ютера приймати, у відповідь на перше повідомлення, друге повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа; код для спонукання комп'ютера визначати, що новий обслуговуючий мережевий вузол не підтримує розширений контекст безпеки, якщо відповідь другого повідомлення оснований на одному успадкованому ключі; і код для спонукання комп'ютера захищати передачу даних на основі одного успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує розширений контекст безпеки.

Обслуговуюча базова мережа 230 з'єднана з обслуговуючою RAN 220 (мережа радіодоступу), яка забезпечує бездротову передачу до віддаленого термінала 210. У архітектурі UMTS/UTRAN, обслуговуюча RAN включає в себе вузол B і RNC (радіосетевий контролер). У архітектурі GERAN, обслуговуюча RAN включає в себе BTS (базова приймально-передавальна станція) і BSC (контролер базової станції). Обслуговуюча базова мережа включає в себе MSC/VLR (мобільний комунікаційний центр/візитний реєстр переміщення) для забезпечення послуги в режимі з комутацією каналів (CS), і SGSN (вузол підтримки обслуговування GPRS) для забезпечення послуг в режимі з комутацією пакетів (PS). Домашня мережа включає в себе HLR (реєстр початкового місцеположення) і AuC (центр аутентифікації).

UE 210 і обслуговуюча базова мережа 230 можуть бути розширені з новими властивостями безпеки для створення розширеного контексту безпеки UMTS (ESC) за допомогою COUNT (значення відліку). 256-бітовий кореневий ключ (K_{ASMEU}) для ESC може бути витягнутий з CK і IK, коли виконується аутентифікація AKA. Кореневий ключ може бути встановлений рівним CK||IK або він може бути витягнутий з використанням більш складного витягання, що приводить до додаткових корисних властивостей безпеки (наприклад, CK і IK не повинні бути утримані). COUNT може бути 16-бітовим значенням відліку, яке підтримується між UE і обслуговуючою базовою мережею. (Примітка: успадкований контекст безпеки UTRAN складається з KSI (3-бітовий встановлений ідентифікатор ключа), CK (128-бітовий ключ шифрування) і IK (128-бітовий ключ цілісності).

Даний винахід забезпечує спосіб плавного повернення до успадкованих вузлів від розширених вузлів. Мобільне обладнання/Користувачське обладнання, яке підтримує ESC, може бути позначене UE+. SGSN і MSC/VLR, які підтримують ESC, можуть бути позначені SGSN+ і MSC/VLR+. ESC є прикладом першого контексту безпеки. (Успадковані SGSN і MSC/VLR вказуються без знаку плюс). Спосіб повернення до успадкованих вузлів не залежить від способу, що використовується для визначення сеансових ключів. Не підтримування ESC є прикладом другого контексту безпеки.

Посилаючись на Фіг. 10, UE+210 і SGSN+ або MSC/VLR+ спільно використовують ESC, яка включає в себе KSI (встановлений ідентифікатор ключа), як використовуваний в цей час в UMTS/GERAN, і кореневий ключ K_{ASMEU} . Сеансові ключі CK_S і IK_S обчислюються з кореневого ключа K_{ASMEU} і параметром (наприклад, значенням відліку) обмінюються між UE+ і SGSN+ або MSC/VLR+ (етап 1010). SGSN+230 або MSC/VLR+ також витягують CK_L і IK_L (етап 1020), які функціонують як успадковані ключі, з K_{ASMEU} і фіксованих параметрів, таких як CK_L і IK_L , криптографічно незалежних один від одного, тобто, популярність CK_L і IK_L , не виявляє K_{ASMEU} .

Під час режиму очікування мобільності, або коли UE+ підключається до нової обслуговуючої мережі (етап 1030), параметри ESC можуть бути переміщені з SGSN+230 або MSC/VLR+ до цільових SGSN 230' або MSC/VLR, які не підтримують ESC. Для мобільності UE+ такого цільового вузла, джерело SGSN+ або MSC/VLR+ включає в себе CK_L і IK_L в елементах інформації (IE), які несуть успадковані IK і CK (тобто в існуючих CK/IK IE) (етап 1040). K_{ASMEU} є новим IE (етап 1050). Значення COUNT також забезпечується для мети забезпечення можливості витягання сеансових ключів (етап 1060). Якщо цільові SGSN і MSC/VLR не підтримують ESC, то вони будуть ігнорувати нові IE і використовувати CK_L і IK_L як успадковані CK і IK.

UE+ включає в своїх повідомленнях для мети відповідну інформацію для обчислення сеансових ключів. UE+ ще не знає чи підтримує мету ESC. Якщо ціль є успадкованим вузлом (наприклад, не розуміє ESC), то вона використовує CK_L і IK_L, прийняті від джерела SGSN+ або MSC/VLR+ як успадкований контекст безпеки UMTS (поряд з KSI/CKSN). Якщо ціль підтримує ESC, то вона може продовжувати використовувати ESC. Цільовий SGSN+ або MSC/VLR+ сигналізує про свою підтримку ESC в UE.

У UMTS, UE+ може приймати SMC (команду режиму безпеки) від RNC, не знаючи, чи підтримує мету ESC (етап 1070). У цьому випадку, UE+ використовує як IK_L так і IK_S для визначення чи підтримується ESC цільовим SGSN (або MSC/VLR) (етап 1080). Більш конкретно, UE+ обчислює MAC для SMC, використовуючи як IK_L так і IK_S. UE+ звіряє обчислений MAC зі значенням MAC, включеним в SMC. Якщо прийнятий MAC рівний обчисленому MAC з IK_S, то ціль підтримує ESC. Якщо прийнятий MAC рівний обчисленому MAC з IK_L, то ціль не підтримує ESC (етап 1090). У іншому випадку, UE+ відхиляє прийняте повідомлення (наприклад, SMC) в зв'язку з недостатністю цілісності.

У GERAN PS, SGSN+ сигналізує про свою підтримку ESC в повідомленні аутентифікації і шифрування. У GERAN CS, якщо безпека забезпечується перед сигналюванням, можливості MSC можуть бути прийняті за допомогою UE+, причому ключ K_C або K_{CI28} GERAN, витягнутий з CK_L і IK_L може бути тимчасово використаний, до можливого перемикання.

Якщо ціль SGSN і MSC/VLR не підтримує ESC, то як ціль, так і UE+ повертаються до використання успадкованого контексту безпеки з CK_L і IK_L як CK і IK.

Альтернативно, ціль може сигналізувати про підтримку ESC в SMC (наприклад, шляхом додання нового IE, що RNC прийнятий від SGSN+ або MSC/VLR+). Якщо ніяка вказівка не прийнята, то UE+ можна вважати повідомленим з успадкованими SGSN і MSC/VLR. Цей варіант поліпшення вимагає внесення змін в RNC (тобто RNC повинен оновлюватися для відправлення SMC з новими IE).

У режимі з'єднання (активному режимі) при мобільності, неможливо визначити для UE+ можливість цільового SGSN (наприклад, SMC не можлива в режимі з'єднання або це приведе до розриву в поточному виклику/сесії, який не є переважним).

Якщо SGSN змінюється в режимі з'єднання, то джерело SGSN включає в себе CK_S і IK_S в успадкованих IE CK і IK. Як цільовий SGSN, так і UE+ мають на увазі, що цільовий SGSN підтримує тільки успадкований контекст через подальше сигналювання (наприклад, в режимі очікування або обслуговуючих запитів або SMC) і буде повернений до успадкованого контексту безпеки з CK_S і IK_S. Ця відмінність від режиму очікування, в якому CK_L і IK_L використовуються успадкованими вузлами як IK і CK. Якщо цільовий SGSN+ підтримує ESC, то він використовує кореневий ключ K_{ASMEU} для витягання ESC як описано вище.

Посилаючись на Фіг. 5, в способі 500, пов'язаному з процедурами підключення UMTS, UE 210 може сигналізувати, що воно підтримує ESC в повідомленні запиту підключення UMTS (етап 510). Сигнал підтримки може бути наявністю нових елементів інформації (IE) в цьому повідомленні. IE можуть містити значення COUNT. Обслуговуюча мережа SN 230, яка не підтримує ESC буде ігнорувати нові IE. Дані аутентифікації (RAND, XRES, CK, IK, AUTN) отримують від HLR/AuC 240 (етап 515). SN можуть вказувати на підтримку ESC в AKA виклику (запиті аутентифікації) до UE (етап 520). UE виконує процедури аутентифікації (етап 525) і повертає відповідь RES в SN (етап 530). Після успішної аутентифікації (етап 530), UE і SN направляють кореневий ключ K_{ASMEU} і сеансові ключі CK_S і IK_S (етап 535). SN направляє сеансові ключі до RAN 220 в повідомленні SMC (команда режиму безпеки) (етап 540). RAN генерує код аутентифікації повідомлення (MAC) за допомогою сеансового ключа IK_S, який направляється в UE в повідомленні SMC (етап 545). UE звіряє MAC (етап 550) з використанням сеансового ключа IK_S, який витягнутий UE (етап 535), і повертає повний індикатор до RAN (етап 555), який направляє його в SN (етап 560). UE тоді здатний захищати передачу даних з використанням сеансових ключів (етап 565).

Посилаючись на Фіг. 6, в способі 600, пов'язаному з очікуванням в процедурі 600 активного режиму, UE 210 направляє повідомлення обслуговуючого запиту, яке включає в себе значення COUNT, до SN 230 (етап 610). UE і SN витягують нові сеансові ключі CK_S і IK_S з кореневого ключа K_{ASMEU} (етап 620). SN направляє сеансові ключі до RAN 220 в повідомленні SMC (етап 630). RAN генерує MAC, який направляється в UE в повідомленні SMC (етап 640). UE звіряє MAC (етап 650), і повертає повний індикатор до RAN (етап 660), який направляє його в SN (етап 670). UE тоді здатне захищати передачу даних з використанням сеансових ключів (етап 680).

Посилаючись на Фіг. 7, в способі 700, пов'язаному з процедурами 700 керування мобільністю (такими, як оновлення області трасування (RAU) або оновлення області місцеположення (LAU), UE 210 направляє повідомлення запиту RAU (або LAU), яке включає в себе значення COUNT до SN 230 (етап 710). Необов'язково, UE і SN можуть витягувати нові сеансові ключі CK_S і IK_S з кореневого ключа K_{ASMEU} (етап 720). SN може направити сеансові ключі до RAN 220 в повідомленні SMC (етап 730). RAN може генерувати MAC, який може бути направлений до UE в повідомленні SMC (етап 740). UE може звіряти MAC (етап 750), і може повертати повний індикатор до RAN (етап 760), який направляє його в SN (етап 770). SN потім відправляє повідомлення прийняття RAU до UE (етап 780). UE тоді здатне захищати передачу даних з використанням сеансових ключів.

Ключі нового рівня доступу (AS) можуть бути згенеровані для кожного переходу від очікування до активного стану. Подібним чином, ключі можуть бути згенеровані при інших подіях. Значення COUNT може бути відправлене в повідомленнях очікування мобільності і в повідомленнях початкового рівня 3, наприклад, Attaches, RAUs, LAU, для очікування, мобільності, або обслуговуючого запиту. SN може перевіряти, що відправлене значення COUNT не було використане до цього, і оновлювати збережене значення COUNT в процесі. Якщо значення COUNT є новим (наприклад, прийняте значення COUNT > збереженого значення COUNT), UE і SN продовжують обчислення нового ключа CK_S і IK_S , використовуючи функцію витягання ключа (KDF), таку як HMAC-SHA256, від кореневого ключа K_{ASMEU} і відправлене значення COUNT. KDF може включати в себе додаткову інформацію, таку як ідентичність вузла RAN для обчислення нового ключа. Якщо перевірка не вдалася (значення COUNT не нове), SN відхиляє повідомлення. Для використання GERAN, коли K_C і K_{C128} обчислюються з CK_S і IK_S , це може бути зроблене таким же чином, як і при обчисленні з CK і IK .

Сеансові ключі (CK_S і IK_S) можуть мати час життя такий, що UE і обслуговуюча мережа зберігають і використовують сеансові ключі, доти, поки або це не є більш необхідним для збереження ключів для відправки трафіка безпечно між UE і мережею (UE переходить в режим очікування), або не створюється новий контекст в одній з подальших подій (наприклад, подія аутентифікації AKA або мобільності).

Процедури, описані вище, можуть бути також використані для плавного повернення до успадкованих вузлів, коли UE+ переходить від E-UTRAN (Фіг. 9) до UTRAN/GERAN. При переході від E-UTRAN до UTRAN/GERAN, Модуль Керування Мобільністю (MME) посилає до SGSN/SGSN+ як 256-бітовий ключ, який називається K_{ACME} , так і пару ключів, які називаються ключем шифрування (CK') і ключем цілісності (IK'), витягнених з K_{ACME} . SGSN буде стосуватися CK' як успадкованого CK і IK' як успадкованого IK , і ігнорувати K_{ACME} , в той час як SGSN+ буде стосуватися K_{ACME} як його K_{ASMEU} і CK' як його CK_S і IK' як його IK . Потрібно відмітити, що MME і E-UTRAN будуть розглядатися як розширена обслуговуюча мережа, оскільки контекст безпеки переданий від E-UTRAN завжди розглядається як розширений контекст безпеки.

Віддалений термінал 210 може містити комп'ютер 800, який включає в себе носій 820 зберігання, такий як пам'ять, дисплей 830 і пристрій 840 введення, такий як клавіатура. Пристрій може включати в себе бездротовий зв'язок 850.

Посилаючись на Фіг. 1, бездротовий віддалений термінал (RS) 102 (або UE) може сполучатися з одним або більше базовим терміналами (BS) 104 системи 100 бездротового зв'язку. Система 100 бездротового зв'язку може додатково включати в себе один або більше контролерів базових терміналів (BSC) 106, і базову мережу 108. Базова мережа може бути з'єднана з Інтернетом 110 і телефонною комутованою мережею загального користування (PSTN) 112 через відповідне підключення. Типовий бездротовий віддалений термінал може включати в себе переносний телефон або портативний комп'ютер. Система 100 бездротового зв'язку може використати будь-який з множини способів доступу, таких як множинний доступ з кодовим розділенням каналів (CDMA), множинний доступ з часовим розділенням каналів (TDMA), множинний доступ з розділенням частот (FDMA), множинний доступ з просторовим розділенням (SDMA), множинний доступ з полярним розділенням (PDMA), або інші способи модуляції, відомі в даній сфері техніки.

Бездротовий пристрій 102 може включати в себе різні компоненти, які виконують функції на основі сигналів, які передаються або приймаються на бездротовому пристрої. Наприклад, бездротова гарнітура може включати в себе перетворювач, виконаний з можливістю забезпечення виведення на основі сигналу, прийнятого через приймач. Бездротові "годинники"

5 можуть включати в себе користувацький інтерфейс, виконаний з можливістю забезпечення індикації на основі сигналу, прийнятого через приймач. Бездротовий сприймаючий пристрій може включати в себе датчик, виконаний з можливістю забезпечення передачі даних до іншого пристрою.

Бездротовий пристрій може сполучатися через один або більше бездротових каналів зв'язку, які основані або іншим способом підтримують будь-які відповідні технології бездротового зв'язку. Наприклад, в деяких аспектах, бездротовий пристрій може сполучатися з мережею. У деяких аспектах, мережа може містити мережу області тіла або мережу персональної області (наприклад, ультра-широкопasmово мережа). У деяких аспектах, мережа може містити локальну мережу або глобальну мережу. Бездротовий пристрій може

15 підтримувати або іншим чином використати одну або більше з множини бездротових комунікаційних технологій, протоколів і стандартів, таких як, наприклад, CDMA, TDMA, OFDM, OFDMA, WiMAX і Wi-Fi. Подібним чином, мобільний пристрій може підтримувати або іншим чином використовувати одну або більше з множини відповідних модуляцій або схем мультиплексування. Бездротовий пристрій, таким чином, може включати в себе відповідні

20 компоненти (наприклад, радіоінтерфейси) для встановлення і сполучення через один або більше бездротових каналів зв'язку з використанням вищезгаданих або інших бездротових технологій зв'язку. Наприклад, пристрій може містити бездротовий приймач-передавач з відповідними компонентами передавача і приймача (наприклад, передавач і приймач), які можуть включати в себе різні компоненти (наприклад, генератори сигналів і процесори

25 сигналів), які сприяють передачі даних через бездротовий носій.

Предмет винаходу може бути вбудований в (наприклад, втілений в рамках або виконаний за допомогою) різні апарати (наприклад, пристрої). Наприклад, в одному або більше аспектах, винахід може бути вбудований в телефон (наприклад, стільниковий телефон), персональний секретар даних ("PDA"), розважальні пристрої (наприклад, музичні або відеопристрої), гарнітуру

30 (наприклад, навушники, головний телефон і т. д.), мікрофон, медичний пристрій (наприклад, біометричний датчик, монітор серцевого ритму, крокомір, пристрій ЕКГ і т. д.), користувацький пристрій введення/виведення (наприклад, годинник, пульт дистанційного керування, вимикач світла, клавіатуру, мишу і інш.), монітор контролю тиску, комп'ютер, пристрій касового термінала, розважальний пристрій, слуховий апарат, телевізійний префікс або будь-який інший

35 відповідний пристрій.

Ці пристрої можуть мати різну потужність і вимоги до даних. У деяких аспектах, винахід може бути пристосований для використання в додатках малої потужності (наприклад, за рахунок використання схем сигналізації на імпульсній основі і режимів з малим робочим циклом) і може підтримувати різні швидкості передачі даних, включаючи відносно високі швидкості

40 передачі даних (наприклад, за рахунок використання імпульсів з великою шириною смуги пропускання).

У деяких аспектах, бездротовий пристрій може містити пристрій доступу (наприклад, Wi-Fi точку доступу) для системи зв'язку. Такий пристрій доступу може забезпечувати, наприклад, підключення до іншої мережі (наприклад, глобальної мережі, такої як Інтернет або стільникова

45 мережа) за допомогою дротового або бездротового каналу зв'язку. Відповідно, пристрій доступу може забезпечити іншому пристрою (наприклад, Wi-Fi терміналу) можливість доступу до іншої мережі або деякі інші функції. Крім того, потрібно мати на увазі, що один або обидва пристрої можуть бути портативними, або, в деяких випадках, відносно не портативними.

Фахівцям в даній галузі техніки буде зрозуміло, що інформація і сигнали можуть бути представлені з використанням будь-якої з множини різних технологій і способів. Наприклад, дані, інструкції, команди, інформація, сигнали, біти, символи і елементарні сигнали, які можуть згадуватися в приведеному вище описі, можуть бути представлені за допомогою напруг, струмів, електромагнітних хвиль, магнітних полів або частинок, оптичних полів або частинок, або будь-якою їх комбінацією.

Фахівцями повинне бути додатково оцінено, що різні ілюстративні логічні блоки, модулі, схеми і етапи алгоритму, описані в зв'язку з розкритими варіантами втілень, можуть бути реалізовані у вигляді електронних апаратних засобів, програмного забезпечення або їх комбінації. Щоб ясно проілюструвати цю взаємозамінність апаратних засобів і програмного

55 забезпечення, різні ілюстративні компоненти, блоки, модулі, схеми і етапи були описані вище загалом з точки зору їх функціональності. Чи буде така функціональність реалізована у вигляді

60

апаратного або програмного забезпечення, залежить від конкретного застосування і конструктивних обмежень, накладених на систему загалом. Фахівці в даній галузі техніки можуть реалізувати описану функціональність різними способами для кожного конкретного застосування, але такі рішення втілення не повинні інтерпретуватися як причина відступу від об'єму даного винаходу.

Різні ілюстративні логічні блоки, модулі і схеми, описані в зв'язку з розкритими тут варіантами втілень, можуть бути реалізовані або виконані за допомогою процесора загального призначення, процесора цифрових сигналів (DSP), проблемно-орієнтованою інтегральною мікросхемою (ASIC), програмованою вентиляційною матрицею (FPGA) або іншого програмованого логічного пристрою, дискретної або транзисторної логіки, дискретних апаратних компонентів або будь-якою їх комбінацією, призначеною для виконання функцій, описаних тут. Процесор загального призначення може бути мікропроцесором, але як альтернатива, процесор може бути будь-яким звичайним процесором, контролером, мікроконтролером або кінцевим автоматом. Процесор також може бути реалізований у вигляді комбінації обчислювальних пристроїв, наприклад, комбінацією DSP і мікропроцесора, множиною мікропроцесорів, одним або більше мікропроцесорами в поєднанні з ядром DSP, або будь-якої іншої такої конфігурації.

Етапи способу або алгоритму, описаного в зв'язку з розкритими тут варіантами втілення, можуть бути реалізовані безпосередньо в апаратних засобах, в програмному модулі, що виконується процесором, або в комбінації з двох. Програмний модуль може знаходитися в оперативній пам'яті, флеш-пам'яті, ПЗП, EPROM пам'яті, EEPROM пам'яті, регістрах, жорсткому диску, знімному диску, CD-ROM, або в будь-якій іншій формі носія зберігання, відомій в даній галузі техніки. Зразковий носій зберігання зв'язаний з процесором, так що процесор може зчитувати інформацію з і записувати інформацію на носій. Як альтернатива, носій зберігання може бути інтегрований в процесор. Процесор і носій зберігання можуть знаходитися в ASIC. ASIC може знаходитися в користувацькому терміналі. Як альтернатива, процесор і носій зберігання можуть знаходитися як дискретні компоненти в користувацькому терміналі.

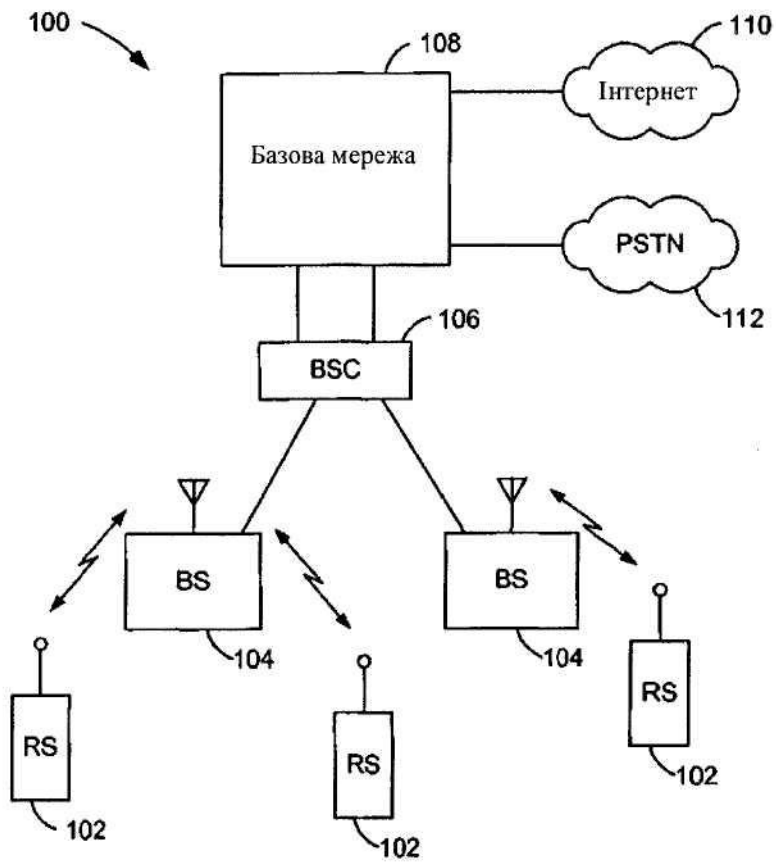
У одному або більше зразкових варіантах втілення, описані функції можуть бути реалізовані апаратними, програмними і програмно-апаратними засобами, або будь-якою їх комбінацією. При реалізації в програмному забезпеченні, як комп'ютерний програмний продукт, функція, можуть бути збережені на або передані, як одна або більше інструкцій або код, в машиночитаний носій. Машиночитаний носій включає в себе як комп'ютерний носій зберігання, так і носій передачі даних, включаючи будь-який носій, який забезпечує передачу комп'ютерної програми з одного місця в інше. Носій зберігання може бути будь-яким доступним носієм, який може бути доступний за допомогою комп'ютера. Як приклад, а не обмеження, такий машиночитаний носій може містити RAM, ROM, EEPROM, CD-ROM або інші засоби на оптичних дисках, засоби зберігання на магнітних дисках або інші магнітні запам'ятовуючі пристрої, або будь-який інший носій, який може бути використаний для виконання або збереження бажаного програмного коду у вигляді інструкцій або структур даних, і який може бути доступний за допомогою комп'ютера. Крім того, будь-яке з'єднання потрібно називати машиночитаним носієм. Наприклад, якщо програма передається з веб-сайта, сервера або іншого віддаленого джерела, використовуючи коаксіальний кабель, волоконно-оптичний кабель, виту пару, цифрові абонентські лінії (DSL) або бездротові технології, такі як інфрачервоні, радіо- і мікрохвильові, то коаксіальний кабель, волоконно-оптичний кабель, вита пара, DSL або бездротові технології, такі як інфрачервоні, радіо- і мікрохвильові включаються у визначення носія. Немагнітний диск і диск, що використовується тут, включають в себе компакт-диск (CD), лазерний диск, оптичний диск, цифровий універсальний диск (DVD), флопі-диски і диски Blu-ray, де диски звичайно відтворюють дані магнітно, в той час як немагнітні диски відтворюють дані оптичним лазером. Комбінації вище, повинні бути також включені в об'єм машиночитаного носія.

Приведений вище опис розкритих варіантів втілення передбачений для забезпечення можливості будь-якому фахівцеві в даній галузі техніки виконати або використати даний винахід. Різні модифікації цих варіантів втілень будуть очевидні для фахівців в даній галузі техніки, і загальні принципи, визначені в цьому документі, можуть бути застосовані до інших варіантів втілень без відступу від суті і об'єму винаходу. Таким чином, даний винахід не обмежується показаними тут варіантами втілення, але повинен відповідати найширшому об'єму відповідно до принципів і нових ознак, розкритих тут.

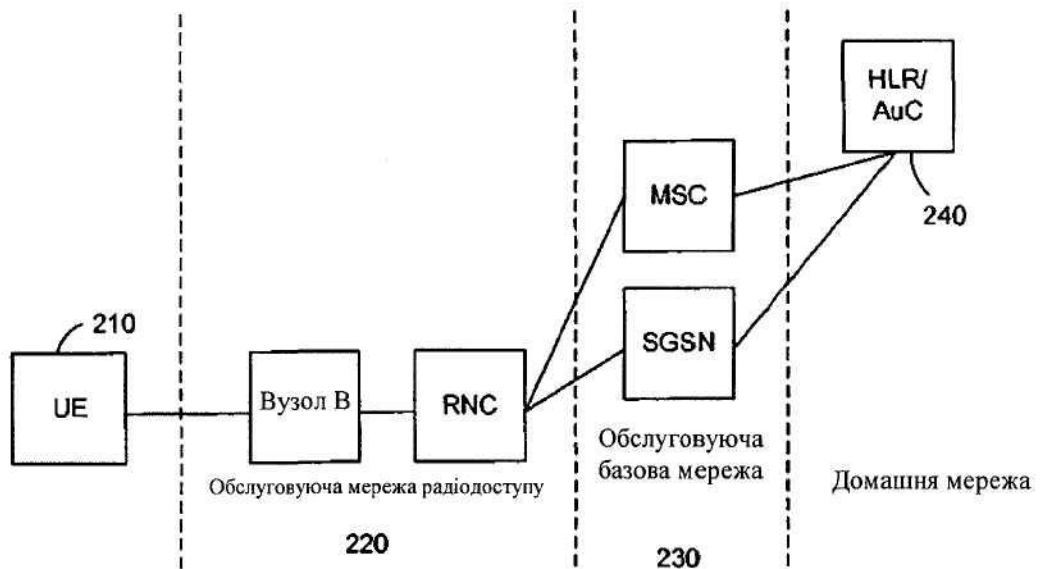
ФОРМУЛА ВИНАХОДУ

1. Спосіб переходу віддаленого термінала від поточного обслуговуючого мережевого вузла, що має перший контекст безпеки, до нового обслуговуючого мережевого вузла, що містить етапи, на яких:
 - забезпечують віддаленим терміналом щонайменше один успадкований ключ, зв'язаний з другим контекстом безпеки, причому перший контекст безпеки включає в себе властивість безпеки, яка не підтримується другим контекстом безпеки;
 - генерують віддаленим терміналом щонайменше один сеансовий ключ, відповідно до першого контексту безпеки, на основі елемента інформації, зв'язаного з першим контекстом безпеки; направляють віддаленим терміналом перше повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе елемент інформації, зв'язаний з першим контекстом безпеки;
 - приймають віддаленим терміналом, у відповідь на перше повідомлення, друге повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа; визначають віддаленим терміналом, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення ґрунтується на щонайменше одному успадкованому ключі; і захищають передачі даних віддаленим терміналом на основі щонайменше одного успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки.
2. Спосіб переходу за п. 1, в якому елемент інформації містить значення відліку.
3. Спосіб переходу за п. 2, в якому значення відліку оновлюється за сеанс.
4. Спосіб переходу за п. 1, в якому перший контекст безпеки є розширеним контекстом безпеки універсальної мобільної телекомунікаційної мережі (UMTS), і другий контекст безпеки є успадкованим контекстом безпеки.
5. Спосіб переходу за п. 1, в якому віддалений термінал містить мобільне користувацьке обладнання.
6. Спосіб переходу за п. 1, в якому друге повідомлення містить код аутентифікації повідомлення (MAC), і віддалений термінал визначає, що відповідь ґрунтується на щонайменше одному успадкованому ключі, за допомогою визначення, що MAC був обчислений з використанням щонайменше одного успадкованого ключа.
7. Віддалений термінал, який містить:
 - засіб для забезпечення щонайменше одного успадкованого ключа, зв'язаного з другим контекстом безпеки, причому перший контекст безпеки поточного обслуговуючого мережевого вузла включає в себе властивість безпеки, яка не підтримується другим контекстом безпеки;
 - засіб для генерування щонайменше одного сеансового ключа, відповідно до першого контексту безпеки, на основі елемента інформації, зв'язаного з першим контекстом безпеки;
 - засіб для направлення першого повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе сигналізацію елемента інформації, зв'язану з першим контекстом безпеки;
 - засіб для прийому, у відповідь на перше повідомлення, другого повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь, ґрунтовану або на щонайменше одному успадкованому ключі, або на щонайменше одному сеансовому ключі;
 - засіб для визначення того, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення ґрунтується на щонайменше одному успадкованому ключі; і
 - засіб для захисту передачі даних на основі щонайменше одного успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки.
8. Віддалений термінал за п. 7, в якому елемент інформації містить значення відліку.
9. Віддалений термінал за п. 8, в якому значення відліку оновлюється за сеанс.
10. Віддалений термінал за п. 7, в якому перший контекст безпеки є розширеним контекстом безпеки UMTS, і другий контекст безпеки є успадкованим контекстом безпеки.
11. Віддалений термінал, який містить:
 - процесор, сконфігурований з можливістю:

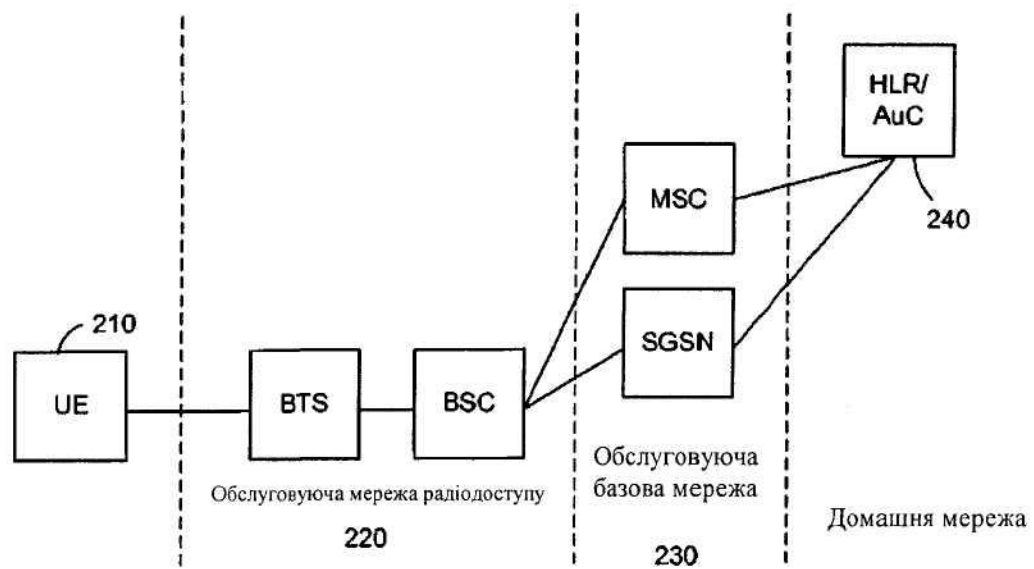
- забезпечення щонайменше одного успадкованого ключа, зв'язаного з другим контекстом безпеки, причому перший контекст безпеки поточного обслуговуючого мережевого вузла включає в себе властивість безпеки, яка не підтримується другим контекстом безпеки;
- 5 генерування щонайменше одного сеансового ключа, відповідно до першого контексту безпеки, на основі успадкованого ключа і елемента інформації, зв'язаного з першим контекстом безпеки; направлення першого повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе елемент інформації, зв'язаний з першим контекстом безпеки;
- 10 прийому, у відповідь на перше повідомлення, другого повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа; визначення, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення оснований на щонайменше одному успадкованому ключі; і захисту передачі даних на основі щонайменше одного успадкованого ключа при визначенні
- 15 того, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки.
12. Віддалений термінал за п. 11, в якому елемент інформації містить значення відліку.
13. Віддалений термінал за п. 12, в якому значення відліку оновлюється за сеанс.
14. Віддалений термінал за п. 11, в якому перший контекст безпеки є розширеним контекстом безпеки UMTS, і другий контекст безпеки є успадкованим контекстом безпеки.
- 20 15. Машиночитаний носій інформації, який містить:
- код для спонукання комп'ютера забезпечувати щонайменше один успадкований ключ, зв'язаний з другим контекстом безпеки, причому перший контекст безпеки поточного обслуговуючого мережевого вузла включає в себе властивість безпеки, яка не підтримується другим контекстом безпеки;
- 25 код для спонукання комп'ютера генерувати щонайменше один сеансовий ключ, відповідно до першого контексту безпеки, на основі елемента інформації, зв'язаного з першим контекстом безпеки;
- код для спонукання комп'ютера направляти перше повідомлення до нового обслуговуючого мережевого вузла, причому перше повідомлення включає в себе елемент інформації, зв'язаний з першим контекстом безпеки;
- 30 код для спонукання комп'ютера приймати, у відповідь на перше повідомлення, друге повідомлення від нового обслуговуючого мережевого вузла, причому друге повідомлення має відповідь на основі або щонайменше одного успадкованого ключа, або щонайменше одного сеансового ключа;
- 35 код для спонукання комп'ютера визначати, що новий обслуговуючий мережевий вузол не підтримує перший контекст безпеки, якщо відповідь другого повідомлення оснований на щонайменше одному успадкованому ключі; і
- код для спонукання комп'ютера захищати передачу даних на основі щонайменше одного успадкованого ключа при визначенні того, що новий обслуговуючий мережевий вузол не
- 40 підтримує перший контекст безпеки.
16. Машиночитаний носій за п. 15, в якому елемент інформації містить значення відліку.
17. Машиночитаний носій за п. 16, в якому значення відліку оновлюється за сеанс.
18. Машиночитаний носій за п. 15, в якому перший контекст безпеки є розширеним контекстом безпеки UMTS, і другий контекст безпеки є успадкованим контекстом безпеки.



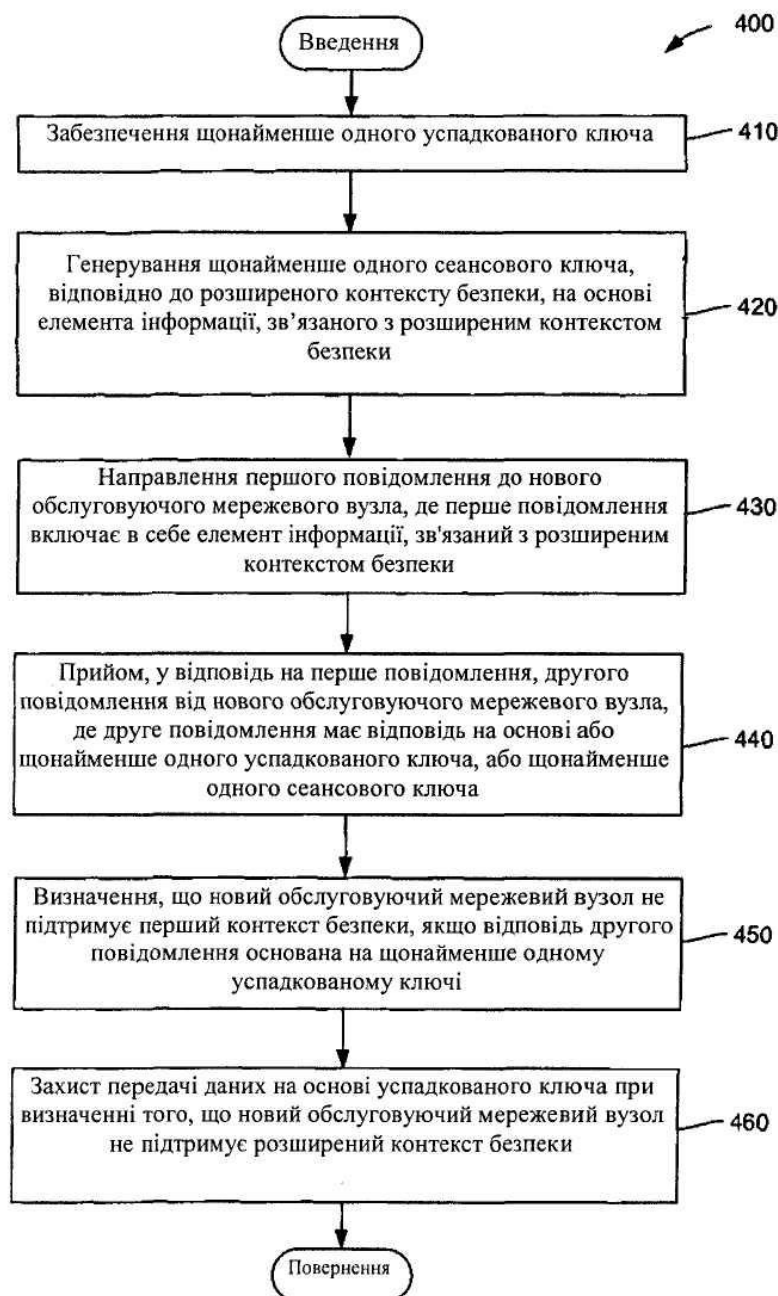
Фіг. 1



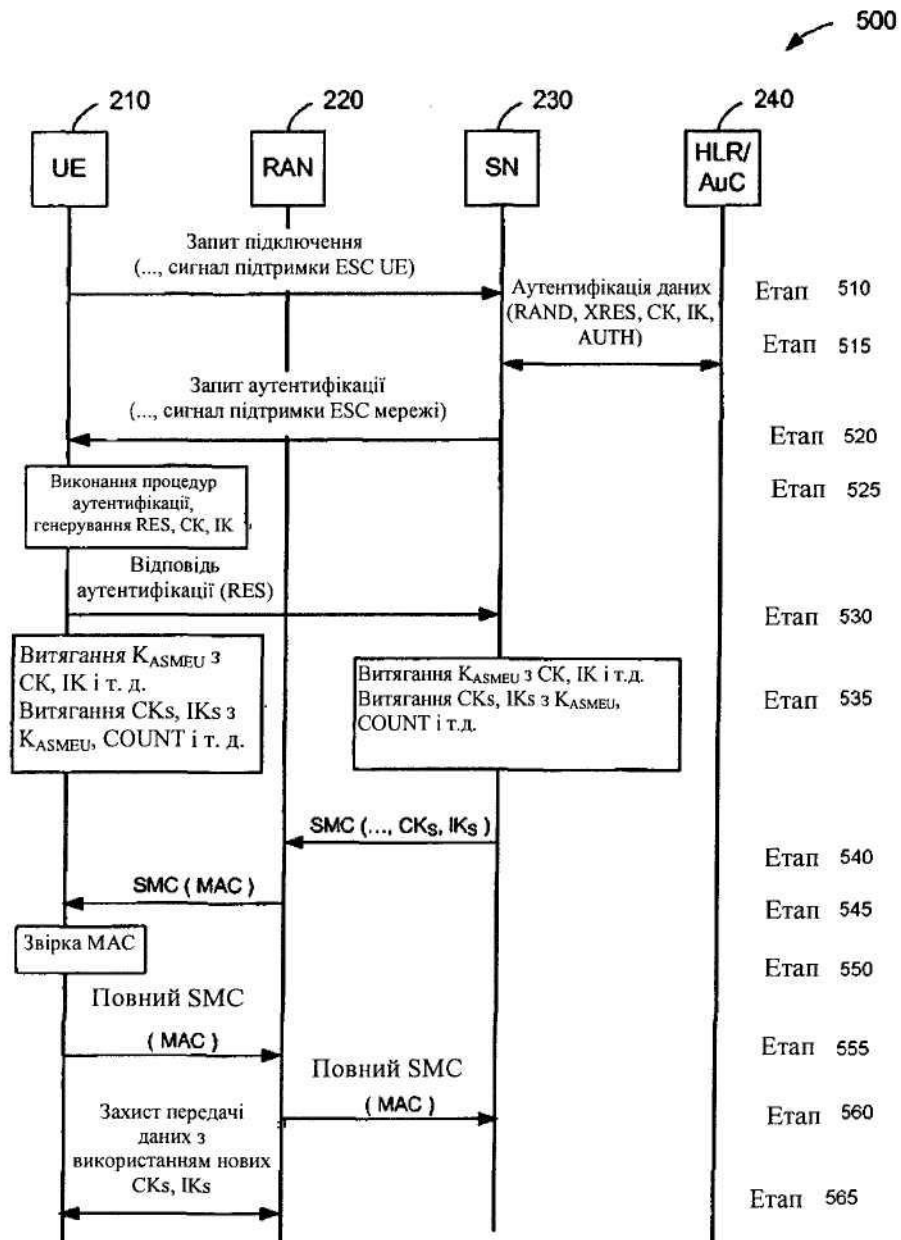
Фіг. 2



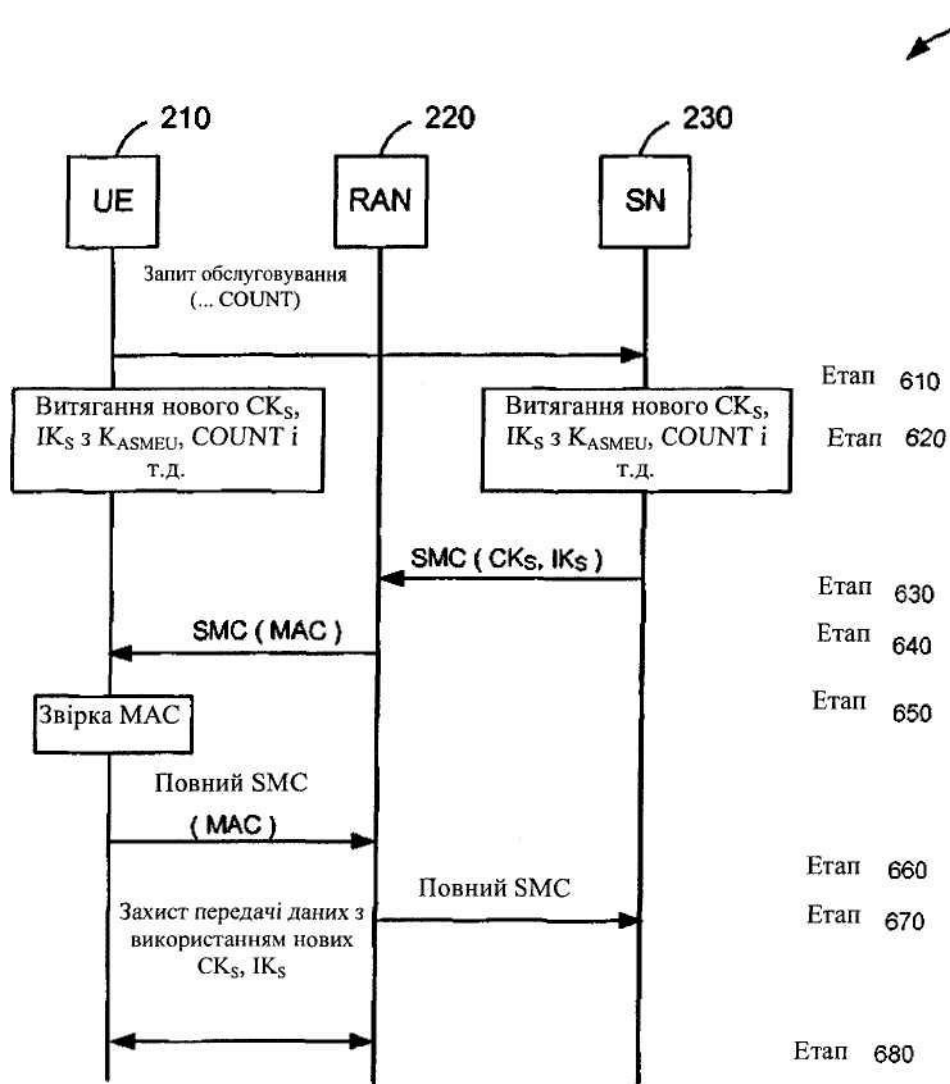
Фіг. 3



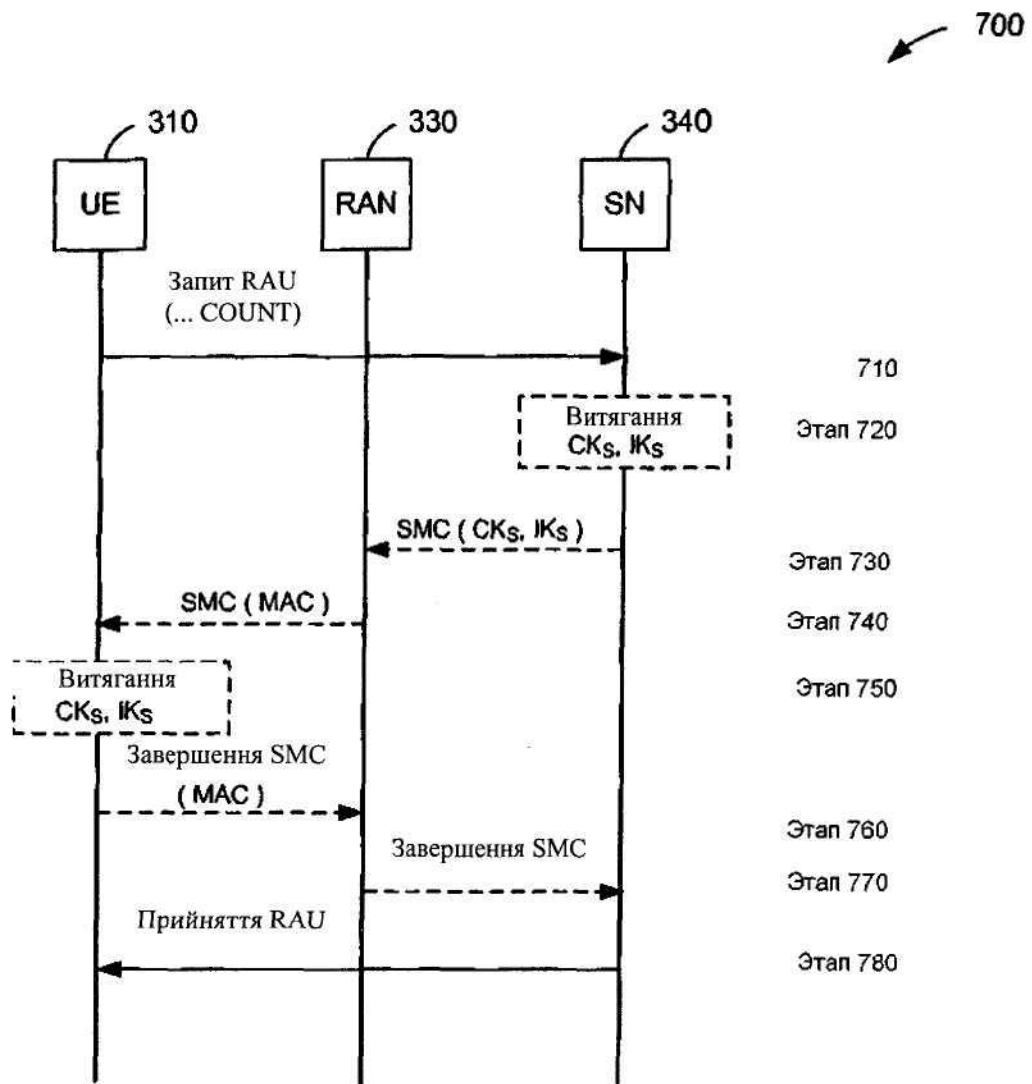
Фіг. 4



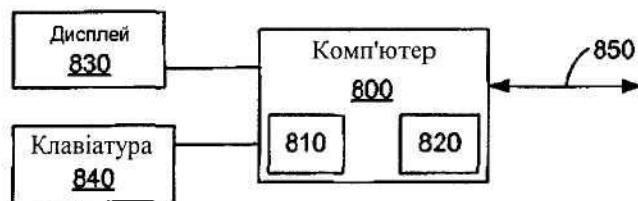
Фіг. 5



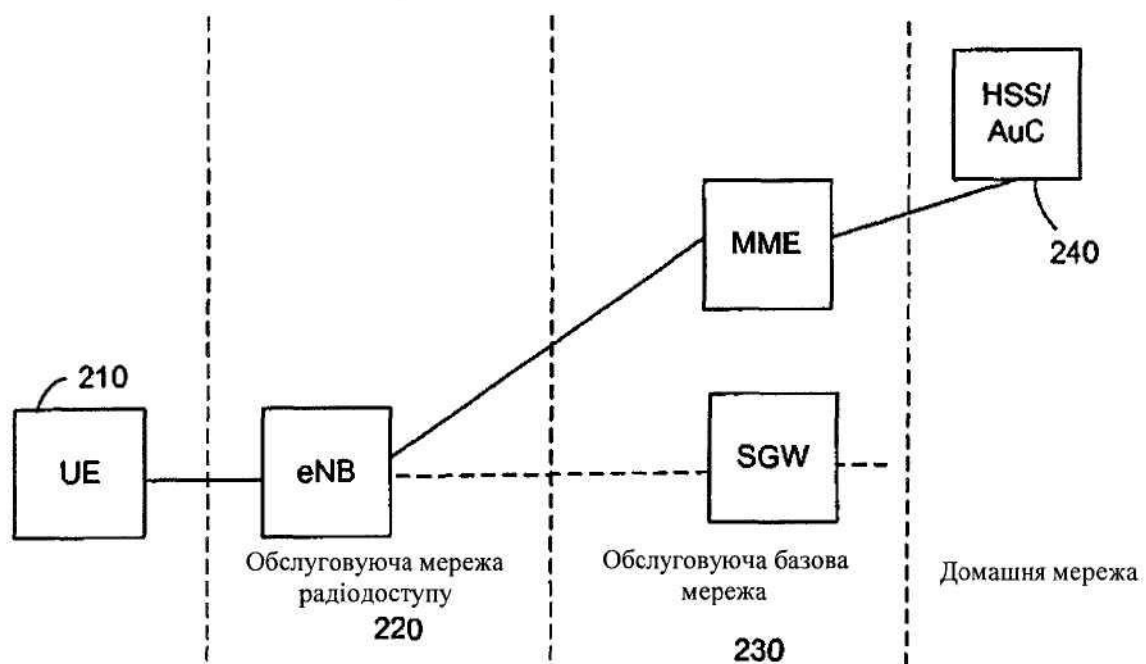
Фіг. 6



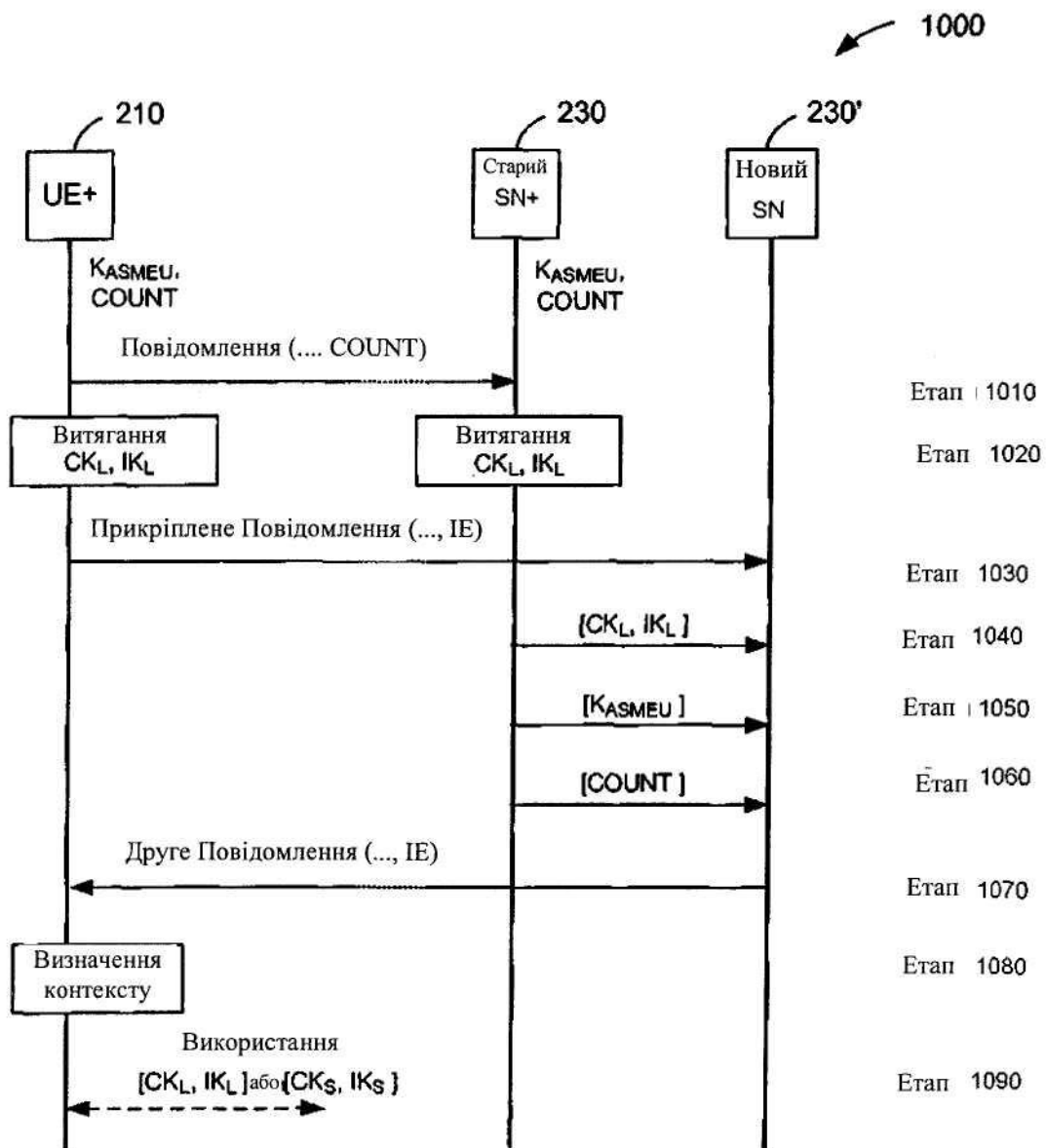
Фіг. 7



Фіг. 8



Фіг. 9



Фіг. 10

Комп'ютерна верстка М. Мацело

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601