(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 770 851**

(51) Int. CI.:

H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.09.2016 PCT/US2016/051696**

(87) Fecha y número de publicación internacional: **23.03.2017 WO17048819**

(96) Fecha de presentación y número de la solicitud europea: **14.09.2016 E 16770186 (1)**

(97) Fecha y número de publicación de la concesión europea: **23.10.2019 EP 3350954**

(54) Título: **Dispositivo y método para criptografía resonante**

(30) Prioridad:

15.09.2015 US 201562218850 P
21.12.2015 US 201514976839

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.07.2020

(73) Titular/es:

GLOBAL RISK ADVISORS (100.0%)
805 Third Avenue
New York, NY 100225, US

(72) Inventor/es:

CHALKER, KEVIN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Dispositivo y método para criptografía resonante

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica la prioridad para la solicitud provisional de Estados Unidos con n.º de serie 62/218.850 presentada el 15 de septiembre de 2015 y la solicitud de Estados Unidos con n.º de serie 14/976.839 presentada el 21 de diciembre de 2015.

Campo de la invención

La tecnología en el presente documento se refiere a la seguridad informática y, más concretamente, a métodos seguros para transferir datos electrónicamente a través de cualquier red. Aún más concretamente, la tecnología en el presente documento se refiere a técnicas de encriptación de datos que usan conceptos de libretas de un solo uso y claves de datos de tamaño pequeño con confianza.

Antecedentes

La criptografía de clave pública ("PKI") se desarrolló por primera vez en la década de 1970 y, hasta la fecha, únicamente ha sido testigo de mejoras paulatinas modestas. Las debilidades conocidas están bien estudiadas, al igual que los fallos sistémicos que dan como resultado pirateos devastadores derivados de los fundamentos frágiles e imperfectos del propio diseño. La razón básica es que PKI es una solución "de mundo perfecto" - solo funciona bien en un entorno libre de errores. La misma falla catastróficamente en el mundo real.

Se conoce la encriptación de datos que usa cifrados de transmisión por secuencias o cifrados de bloques. Los cifrados de transmisión por secuencias y de bloques se usan ampliamente, aunque no es matemáticamente demostrable que sean seguros al 100 %. Estos pueden usar criptografía asimétrica (o de clave pública). Las claves son habitualmente de un tamaño fijo y pueden ser estáticas. Se realiza un cálculo, a cada lado, para encriptar o desencriptar los datos. En un escenario de clave pública habitual, un remitente usa la clave pública de un par de clave pública y clave privada para encriptar un mensaje. El receptor usa la clave privada correspondiente para desencriptar el mensaje. Se proporciona seguridad ya que, en general, es computacionalmente inviable obtener la clave privada a partir de la clave pública.

Estos cifrados modernos son inferiores, incluyendo la criptografía de curvas elípticas ("ECC"), AES, RSA, etc., ya que los mismos son vulnerables a un ataque por fuerza bruta contra el espacio de claves, si bien durante un periodo de tiempo prolongado usando ordenadores potentes. Con el advenimiento de los ordenadores cuánticos en desarrollo en la actualidad, el tiempo para desencriptar estos sistemas modernos usando estas técnicas se puede reducir enormemente. En agosto de 2015, una advertencia de la NSA confirmó el riesgo futuro inmediato de usar estos sistemas y lo recomendó contra el uso de ECC. Recomendaciones adicionales confirmaron que toda esta clase de sistemas criptográficos adolecía del mismo riesgo y no se podría usar como base para asegurar información.

Las libretas de un solo uso se inventaron a principios del siglo XX y son el único sistema criptográfico seguro de manera demostrable que también era invulnerable al ataque por ordenadores cuánticos. Normalmente, estos están reservados para los requisitos de comunicación más seguros. La encriptación de Libreta de un Solo Uso ("OTP") usando claves aleatorias puede producir un secreto perfecto demostrable. De hecho, cualquier sistema criptográfico con secreto perfecto ha de usar estructuras de claves similares a OTP para ser resistentes al análisis criptográfico y al ataque por fuerza bruta. Incluso los ordenadores cuánticos, mencionados anteriormente, tendrán un impacto nulo sobre los sistemas criptográficos basados en OTP.

En un escenario de OTP manual, el remitente tiene una libreta de papel en la que se escriben letras clave elegidas aleatoriamente. La clave es del mismo tamaño que el mensaje. En una implementación, el remitente añade una letra clave a cada letra de texto sin formato para producir texto de cifrado, y nunca repite las letras clave. Por ejemplo, supóngase que el mensaje es "SÍ" y las letras de libreta son "CMG". Se añadiría Y (25) a C (3) para obtener B ((25 + 3) módulo 26 = 2), o E (5) a M (13) para obtener R (18). El remitente destruye entonces el papel. El receptor invierte el proceso usando su libreta de papel (la encriptación es, por lo tanto, simétrica), y quema entonces las letras clave cuando ha acabado. Debido a que la clave tiene el mismo tamaño que el texto sin formato, cada texto sin formato posible es igualmente probable y es imposible que un atacante sepa cuándo se ha obtenido la desencriptación correcta. No es posible un ataque por fuerza bruta contra el espacio de claves completo. Véase, por ejemplo, Schneier, *Secrets and Lies*: *Digital Security In a Networked World* (Wiley Publishing, 2000).

Algunos cifrados de transmisión por secuencias intentan aproximarse a una operación de pseudo-OTP. En tales escenarios, el transmisor y el receptor generan, de forma independiente pero síncrona, la misma clave. Debido a que las claves son calculadas y no son verdaderamente aleatorias, estas se pueden vulnerar a veces (la clave no es segura ya que es calculada) pero pueden proporcionar la seguridad adecuada dependiendo del contexto y de los

algoritmos criptográficos usados. Los cálculos de cifrado de transmisión por secuencias pueden llevar, a veces, un tiempo considerablemente mayor que una única operación de adición o de O exclusivo, como se usa en ciertas implementaciones de libreta de un solo uso, pero este tiempo de cálculo puede tener diferentes impactos dependiendo del contexto.

El documento de publicación de solicitud de patente de Estados Unidos US 2004/161106 A1 a nombre de Matsuda y col. divulga un sistema para comunicaciones seguras usando criptografía, que comprende un generador de números aleatorios que comprende al menos uno de un generador de números aleatorios verdaderos, un generador de números pseudoaleatorios y cualquier secuencia no repetitiva de números que tenga una característica de una secuencia de números aleatorios, y generar una primera secuencia de números aleatorios; y un transmisor, acoplado eléctricamente al generador de números aleatorios, que transmite la primera secuencia generada de números aleatorios.

El documento de publicación de patente de Estados Unidos 6.052.786 a nombre de Tsuchida divulga una unidad de encriptación que comprende varios generadores de números aleatorios que se están usando como un generador de secuencias clave.

El documento de publicación de solicitud de patente de Estados Unidos US 2009/060180 A1 a nombre de Schneider divulga una pluralidad de generadores de números aleatorios Blum-Blum-Shub que trabajan juntos para generar una secuencia clave única y fuerte.

El documento de publicación de solicitud de patente de Estados Unidos US 2015/229621 A1 a nombre de Kariman y col. divulga un método y aparato para generar una libreta de un solo uso usando una pluralidad de generadores de números aleatorios.

El documento de publicación de solicitud de patente de Estados Unidos US 2014/0333416 A1 a nombre de Eichholz y col. divulga la transmisión de una clave criptográfica a través de una conexión de corto alcance.

Existe una serie de obstáculos importantes para implementar con éxito un sistema de OTP, incluyendo el almacenamiento y la distribución de claves, la reposición de materiales de clave, etc. Más allá del secreto perfecto, los beneficios prácticos potenciales son: complejidad simplificada de hardware y software; costes menores de energía y de recursos informáticos - a niveles de CPU, dispositivo, sistema y red; velocidad de ejecución extremadamente alta en los modos de cifrado tanto de secuencias como de bloques; acceso ampliamente expandido a la seguridad para sensores y dispositivos electrónicos simples.

Habitualmente, las OTP se crean usando Generadores de Números Aleatorios ("RNG") y se distribuyen desde una única ubicación a los destinatarios autorizados en formato digital o de papel. En los sistemas criptográficos de OTP, las claves de longitud variable usadas para encriptar mensajes son al menos tan largas como los propios mensajes (indicado anteriormente), lo que difiere de los sistemas criptográficos que usan claves de longitud fija y algoritmos matemáticos complejos. Adivinar la clave de OTP correcta usada para crear un texto de cifrado es posible pero inútil en última instancia, ya que no hay forma de saber que se ha recuperado el texto sin formato correcto. Cualquier número de claves adivinadas puede producir cualquier número de texto sin formato válido sin relación alguna con el texto sin formato de destino. A la inversa, cualquier número de mensajes de la misma longitud encriptados con el mismo sistema de OTP, usando todos ellos unas claves completamente diferentes, pueden producir exactamente el mismo texto de cifrado. En este sentido, adivinar correctamente una de las claves no acerca más al analista criptográfico a recuperar el texto sin formato de interés. No ataque por fuerza bruta posible alguno contra el espacio de claves y, de forma más esencial, contra el propio sistema criptográfico.

La convergencia en un sistema criptográfico demostrablemente seguro es más importante que nunca ya que el Internet de las cosas ("IoT") está cambiando en la actualidad el panorama de la tecnología informática y transformará de forma fundamental la forma en la que pensamos acerca del movimiento de datos. El tráfico anual basado en IP superará, por sí solo, la escala de los Zettabytes en 2016, lo que requerirá una cantidad proporcional de infraestructura de seguridad para protegerlo (un zettabyte = mil millones de terabytes, un número imposiblemente grande como para que la mente humana lo comprenda).

Decir que es deplorable lo inadecuado de la arquitectura de seguridad actual para abordar el desafío supone quedarse muy corto, ya que no se da cuenta de la proliferación de las emergentes transmisiones de datos no basadas en IP y de las nuevas comunicaciones en el horizonte cercano. Ampliar los sistemas existentes para encriptar y asegurar completamente estas estructuras de red en evolución sería, como mínimo, un problema colosal de ingeniería y de diseño que consiste en innumerables partes móviles y miles de horas de trabajo en investigación y desarrollo. Los sistemas complejos se descifran y se ven puestos en peligro de formas complejas que rara vez son entendidas o apreciadas por sus ingenuos creadores. La esencia del pirateo contemporáneo se basa en este principio y solo crece con la complejidad técnica - un paradigma insostenible para el IoT, que promete un crecimiento enorme entre la conectividad de sistemas dispares de dispositivos.

Obsérvese que, para los sistemas modernos, cuanto más larga sea la longitud de la clave, más segura se considera

esta. Sin embargo, cuanto más larga sea la clave, o cuanto más compleja sea la computación para resolver la clave, se requiere una potencia informática cada vez mayor. Ya que se requiere que los datos procedentes de cada vez más dispositivos en el IoT estén encriptados y sin encriptar, se requiere cada vez más energía, lo que supone una carga para las baterías de los dispositivos no cableados. Es necesario un tamaño (o "peso") de clave reducido y / o un protocolo de cómputo simplificado, pero conservando la totalidad de la seguridad robusta.

Reducir la complejidad y aumentar la seguridad requiere comenzar en infinito menos delta y avanzar hacia atrás. La OTP, a diferencia de los sistemas modernos como AES-256 y ECC, solo se puede vulnerar si la implementación fuera defectuosa, mientras que una implementación adecuada es invulnerable con independencia de los recursos informáticos disponibles, ya sean cuánticos o no. Irrumpir en todos los sistemas existentes tendrá lugar con suficientes recursos, mientras que la OTP es invulnerable a los avances informáticos derivados de la ley de Moore. La OTP es también "ligera" y se puede calcular usando algoritmos simplificados.

Más allá de la criptografía, pero parte del trasfondo del concepto inventivo, es el de las redes de sincronización y resonancia natural. En la física y en la naturaleza, dos (o más) entidades resuenan cuando una envía una señal que hace que la otra vibre (oscile) a la misma frecuencia. Esta señal se puede transferir de forma simultánea a través de muchos miembros de un grupo, por lo que se dice que todos ellos están en "resonancia". Se produce un ejemplo cuando un cantante da la nota exacta necesaria para hacer vibrar una copa de vino para que "cante" la misma nota (oscile a la misma frecuencia). O cuando se afina un piano o guitarra a la misma frecuencia de un tono de diapasón que vibra.

En la mecánica cuántica y en la teoría de cuerdas, solo se permiten ciertos tipos de vibraciones, que es lo que, a un nivel fundamental, son todas las partículas y fuerzas - las vibraciones no permitidas no pueden existir. También hay ejemplos biológicos, tales como las luciérnagas Pteroptyx, que llenan árboles grandes con millones de ejemplares que emiten pulsos al unísono, tal como si todas ellas fueran una luz gigantesca aunque son insectos separados. Esto no sucede de forma instantánea, y los diferentes grupos emiten pulsos a tasas diferentes y en momentos diferentes. El "acoplamiento" se produce cuando un grupo y un insecto particular tienen oscilaciones simpáticas - desde la perspectiva de un observador distante, estos son como dos luces estroboscópicas al armonizarse. La propia frecuencia de pulso del insecto se "acopla" a la del grupo. El grupo queda sincronizado con el sustrato de estos osciladores acoplados (los insectos), formando una red de sincronización.

Volviendo atrás, los sistemas de encriptación de clave pública centralizados en el núcleo de los protocolos de seguridad global de Internet son inadecuados para el IoT y las tecnologías emergentes en el horizonte cercano. El cuidado y la alimentación de la infraestructura compleja requerida para su mantenimiento han fallado de forma consistente, lo que ha dado como resultado pirateos de grandes corporaciones e individuos por igual. Con el advenimiento de los ordenadores cuánticos en los próximos años, es vulnerable a los ataques por fuerza bruta y es necesario su reemplazo por un paradigma criptográfico más potente.

Sumario

La presente invención se define en las reivindicaciones adjuntas.

La Criptografía Resonante ("RC") es una tecnología sumamente escalable, exponencialmente más segura y dispersa que reemplazará la dependencia actual en herramientas arcaicas, bosquejadas por primera vez hace más de dos generaciones. Esta impulsará la seguridad de red hacia abajo hasta la capa de niebla, en donde los dispositivos interaccionan directamente y desarrollan una red sumamente resistente de conectividad global segura. Esta será la Espuma Criptográfica.

La batalla para hacer dispositivos / hardware / software perfectamente seguros ya se ha perdido. Las herramientas basadas en firma de los cortafuegos y software antivirus han fallado ya que no pueden predecir el perfil futuro de las infecciones. La mayoría de estas tecnologías han convergido en la actualidad y los diferentes proveedores comerciales son en gran medida indistinguibles. En consecuencia, el software antivirus, los cortafuegos, etc., son un negocio moribundo - las características y ventajas diferenciadoras entre las empresas se han perdido, en gran medida, por competición. No existe combinación única alguna de herramientas de seguridad apiladas en una alineación perfecta. La base del enfoque moderno del director de seguridad de la información (CISO) es la vieja idea de "cómo de rápido has de ser para huir corriendo del ataque de un oso". Mi empresa ha de ser un objetivo más difícil que mi competidor más cercano. Sin embargo, si su empresa es una entidad objetivo prioritaria a toda costa, por ejemplo, por un actor estatal decidido y bien financiado, se desplegarán recursos crecientes para irrumpir en la red normalmente reservada para los objetivos más difíciles.

El modelo de RC invierte en esencia el paradigma de seguridad - la suposición es que el software y el hardware siempre serán defectuosos y vulnerables, pero cuando estos se acoplan a múltiples secuencias de datos aleatorizantes que ofuscan su actividad, los mismos son inherentemente más difíciles de atacar y, en consecuencia, exponencialmente más seguros. El análisis de patrones y firmas en busca de defectos y debilidades es derrotado por una difusión de ruido aparente. Todas las comunicaciones y contenidos seguros parecen ser secuencias de números aleatorizados que solo varían en cuanto a su longitud.

La RC es un enfoque radicalmente diferente a la criptografía y a la seguridad para todas las comunicaciones, en especial los sistemas basados en IP y más allá, y es ideal para el IoT. La RC crea un entorno de generadores de señales de números aleatorios, un subconjunto de los cuales puede ser recibido por dispositivos de usuario que acuerden comunicarse. Estas señales acordadas se usan de la misma manera en la que funciona una libreta de un solo uso, para encriptar de forma instantánea los datos entre los usuarios o entre grupos de usuarios. Esto es encriptación de secuencias, no encriptación de bloques, pero se puede implementar en cualquier formato.

En la RC, no se requiere ninguna autoridad central de claves o sistema complejo de infraestructura criptográfica, lo que significa que ningún actor tiene una puerta trasera universal y es virtualmente imposible de vulnerar (más fuerte que AES o ECC). La RC empuja la seguridad de las comunicaciones al borde de red, en donde los dispositivos interaccionan usando recursos informáticos decrecientes necesarios para asegurar un sistema. La RC requiere muchos menos recursos informáticos en los dispositivos móviles para la encriptación y, por lo tanto, usa mucha menos energía al tiempo que casi elimina la latencia asociada con la encriptación (un problema central de las baterías en todas las tecnologías informáticas móviles modernas).

La RC involucra una colección de dispositivos denominados resonadores criptográficos que envían una señal de IP constante de números aleatorios, de forma análoga a una estación de radio de Internet. En algunos ejemplos, estas son secuencias estáticas, otros ejemplos permiten que los resonadores criptográficos respondan a su entorno y al número de usuarios en el sistema.

Los ejemplos de RC usan una red distribuida de resonadores criptográficos para crear secuencias de OTP para encriptar las comunicaciones. Los dispositivos pueden acceder a una o más de estas secuencias continuas para crear una OTP única usada en esquemas de encriptación simétricos o asimétricos en configuraciones de cifrado de bloques o de cifrado de secuencias. En otros ejemplos, múltiples secuencias se pueden combinar de formas complejas para producir unas OTP inimitables con una entropía alta. Estas secuencias de resonador criptográficos también se pueden incrustar de manera reactiva fuera de las secuencias de datos, o bien aleatorias o bien no aleatorias, dependiendo del fin. Múltiples dispositivos se pueden comunicar de manera segura o "resonar" criptográficamente al acordar el uso de unas OTP específicas. Se puede establecer un canal encriptado seguro cuando todos los participantes están en un estado de resonancia entre sí y las OTP seleccionadas.

Usando como ejemplo la nomenclatura convencional, Alice quiere comunicarse con Bob en secreto. Antiguamente, cada uno de ellos hubiera tenido una OTP con una lista muy larga de números aleatorios que se podían usar para encriptar y desencriptar un mensaje. Cuando se acabara la lista, obtendrían una libreta nueva y comenzarían desde el principio. Esto es una encriptación perfecta ya que no hay forma de adivinar el orden de los números en su OTP. Con la RC de la presente invención, ahora pueden hacer lo mismo. Cada uno de ellos podría acordar "acoplarse" a un conjunto particular de resonadores criptográficos, en un determinado momento o lugar, que están transmitiendo por secuencias, continuamente, números aleatorios. Dado que estos acuerdan que esta secuencia única de números es la "clave" efectiva para su sistema criptográfico, han comenzado a comunicarse con la libreta de un solo uso de la invención.

Nunca reutilizan parte alguna de la clave ya que esta está cambiando constantemente de nanosegundo a nanosegundo. Nadie necesita ser el maestro de claves y Alice y Bob se pueden comunicar de forma segura sin que un tercero intermedie en el intercambio criptográfico. Este es un intercambio de secreto de igual a igual sin tener que almacenar o proteger una clave secreta. Hay muy poco riesgo de que alguien adivine las combinaciones correctas de tiempo, espacio, resonadores, etc., que usaron Alice y Bob y no tiene sentido almacenar cada combinación posible, ya que esto se convierte rápidamente en un problema informático inabordable conocido como NP-complejo. Este es significativamente más difícil de descifrar que AES o sus equivalentes y es resistente al ataque incluso por los ordenadores cuánticos futuros, lo que no son todos los algoritmos usados en la actualidad para la criptografía de clave pública. En este sentido, la RC es inconmensurablemente más segura.

Otros ejemplos permiten que los dispositivos reciban de forma pasiva la secuencia o secuencias de resonador criptográficos para crear unas OTP únicas, alertando o sin alertar a la red de que esas secuencias están en uso. Estas pueden ser radiodifusiones públicas o privadas efectivas de estas secuencias de resonador criptográficos y pueden estar disponibles libremente, por abono / pertenencia o uso exclusivo y cualquier variante de los mismos. Los dispositivos se pueden conectar directamente o a través de entidades representantes.

Los dispositivos pueden tener sus propios resonadores criptográficos que se pueden acoplar con la red de resonadores criptográficos al perturbar los resonadores criptográficos de red con los resonadores criptográficos transmitidos por el dispositivo, para aumentar adicionalmente la entropía y crear un estado enmarañado entre la red y los dispositivos que la usan para encriptar las comunicaciones. Cualquier dispositivo también se puede conectar directamente a otros dispositivos con resonadores criptográficos de dispositivo.

Cualquier elemento en la red puede responder a cualquier dispositivo al incorporar una señal única a partir del dispositivo, lo que puede alterar de forma detectable uno o más de los resonadores criptográficos. Esto es equivalente a una señal a otros dispositivos con conocimiento de esta firma única, que puede parecer idéntica, o no,

a la secuencia de resonadores criptográficos ordinaria. Esta se puede usar por cualquier número de razones más allá de la señalización, incluyendo iniciar una sesión segura, marcar el bloque de OTP exacto a usar, etc.

Las secuencias se pueden almacenar en memoria intermedia o capturar para su inclusión recursiva en cualquier secuencia de resonador criptográficos en vivo. Esta recursividad crea un lazo de realimentación de secuencias históricas de resonadores criptográficos que afectan a las secuencias en vivo de una manera dinámica. Esto se puede lograr mediante el entrelazado simple de secuencias de números aleatorios a técnicas de aleatorización complejas para fusionar las secuencias de datos de resonadores criptográficos históricos y en vivo. Esto se puede usar para múltiples fines, incluyendo el aumento de la entropía, la señalización y el enmarañamiento.

Se pueden recombinar una o más redes de resonadores criptográficos primarios y una pluralidad de resonadores criptográficos de dispositivo para crear secuencias secundarias y terciarias de unas OTP asignadas dinámicamente o como una transmisión estática y regular. Estas secuencias recombinantes se pueden usar para crear resonadores criptográficos nuevos y dar servicio a esquemas recursivos.

Otros ejemplos permiten que un conjunto dinámico de datos encriptados en vivo se facilite de forma pública o privada con cada entrada encriptada por una OTP única, usando resonadores criptográficos de red o de dispositivo. Cada punto de datos resuena con la misma OTP accesible por los espectadores autorizados. Un único conjunto de datos puede reaccionar a múltiples OTP para crear unos niveles escalonados de controles de acceso sobre los datos, en donde algunos usuarios solo pueden ver un subconjunto del conjunto de datos completo.

En un ejemplo de valla geográfica, se pueden usar resonadores criptográficos o constelaciones de resonadores criptográficos aislados física o lógicamente para establecer un perímetro criptográfico o "valla geográfica" en torno a un grupo de dispositivos de usuario autorizados. Todas las comunicaciones y datos dentro de esta valla geográfica son acoplados y encriptados por un conjunto único de OTP obtenidas de estos resonadores criptográficos que no son accesibles por nadie fuera de la valla geográfica. La frontera de este conjunto de resonadores criptográficos sirve como un punto de control efectivo para la entrada / salida a una red encriptada cerrada. Estos perímetros criptográficos se pueden superponer y tener fronteras compartidas que soportan esquemas de autorización de acceso complejos.

La señal de un resonador criptográfico se puede alterar de manera no aleatoria al fusionarla con una segunda secuencia de datos secreta en el dispositivo de resonadores criptográficos creando una "señal fantasma" y una capa de ofuscación de datos nueva. Aunque los resonadores criptográficos continúan difundiendo una secuencia de números aparentemente aleatorios, esta porta entonces una señal fantasma incrustada que puede ser detectada por destinatarios autorizados usando el filtro correcto para distinguirla de la secuencia normal de resonadores criptográficos. La señal fantasma puede ser un conjunto de datos o un conjunto separado de resonadores criptográficos a usar como una OTP o con una OTP.

Usando uno de los anteriores, o todos ellos, se pueden crear y usar series de OTP para encriptar y archivar datos que no cambiarán con el tiempo. La OTP única se crea y almacena durante una ventana en el tiempo asociada con el conjunto de datos de una serie de resonadores criptográficos existentes en la misma ventana de tiempo.

En profundidad, parte de la red de resonadores criptográficos se puede conectar a Internet y puede ser accesible a través de cualquier conexión desde cualquier lugar, a través de VPN o de otra manera. Estos pueden ser conexiones cableadas o inalámbricas, el único requisito es el acceso directo a Internet o a un sistema de comunicaciones similar. Otros pueden estar completamente desconectados de Internet y equivaler a balizas de radio accesibles por Bluetooth, Zigbee, NFC, WiFi, LiFi, IR, etc. Otros ejemplos más de los resonadores criptográficos pueden ser señales móviles conectadas a dispositivos de usuario, coches y virtualmente cualquier cosa que se mueva, incluyendo satélites y submarinos. Los usuarios se pueden encontrar y conectar entre sí mediante casi cualquier aplicación que exista en la actualidad - número de teléfono, dirección de correo electrónico, Facebook, Twitter, etc. Esto mismo es válido para conectarse a redes y dispositivos o en grupos, no se limita a las comunicaciones de persona a persona. Es la tecnología de seguridad suprema que podría conectar cualquier cosa de manera efectiva y segura, no solo ordenadores.

De la misma manera que el GPS usa datos de múltiples satélites para ubicar geográficamente un dispositivo, un grupo de comunicadores seguros puede acordar acoplar un conjunto específico de resonadores de forma simultánea - compartiendo en la práctica la misma OTP. Esta puede ser cualquier combinación de resonadores públicos y privados accesibles por todos o solo unos pocos de tipo privado (por abono o diseño). Se pueden basar en la ubicación geográfica o en la conexión lógica a través de Internet. La relación exacta es irrelevante, salvo por que todos ellos tienen acceso continuamente a la misma señal criptográfica. En las situaciones en las que la proximidad es obvia, tal como en el caso de todas las personas dentro del edificio de una empresa, esto es trivial. Una serie de resonadores de tipo baliza desconectados de Internet es suficiente para asegurar todas las comunicaciones en el edificio, ya que un observador distante no puede confiar en capturar todas estas señales de baja potencia, incluso si están al otro lado de la calle. Esto funcionará de sala a sala y de piso a piso para las comunicaciones "de valla geográfica". Es autolimitante, ya que un solo dispositivo puesto en peligro que transmite una señal más allá del edificio no ayuda a un oyente clandestino ya que está cifrado de manera imposible - hay pocas formas de diferenciar

secuencias de números aleatorios. Por ejemplo, un teléfono celular usado para la comunicación corporativa dentro de un edificio se puede transmitir fácilmente a la torre de telefonía celular más cercana, pero las comunicaciones internas, incluso si son capturadas por el dispositivo y difundidas de nuevo, solo envían texto o VoIP encriptada. La desencriptación a texto sin formato solo tiene lugar en los puntos de extremo en donde residen los usuarios de confianza. Cualquier cosa que se capture en pleno vuelo está encriptada.

La potencia, la computación y otros recursos que se ahorran en los ejemplos de la presente invención son obvios. En lugar de mantener unos sistemas de seguridad centralizados y constantemente actualizados con las autoridades de certificación y los administradores de red, la seguridad de la infraestructura y las comunicaciones se puede mejorar enormemente a un menor coste con un riesgo comprobado fundamental menor - no existe autoridad central alguna que atacar y poner en peligro para irrumpir en una entidad. Los usuarios de RC no necesitan alertar a los generadores de RC de que se están usando sus señales.

Se pueden implementar algoritmos simples de uso poco intensivo de CPU y, por lo tanto, de ahorro de energía, para aumentar adicionalmente la seguridad y personalizar las soluciones para diferentes aplicaciones, clientes y bases de usuarios. Por ejemplo, la OTP combinada puede no ser una adición falsa simple de múltiples secuencias de números de resonadores. Cualquier mezcla de las secuencias servirá, como desplazar una secuencia unos pocos milisegundos o realizar operaciones matemáticas simples sobre cualquier combinación de las secuencias para crear un producto criptográfico único. Hacer que una secuencia parpadee de vez en cuando o multiplicarla por un número primo grande son todas las opciones. Se podrían usar técnicas similares para crear una jerarquía de privilegios en una sola sesión - algunos participantes verán todo un comunicado y otros solo verán / oirán una fracción del mismo.

Existen ventajas inmensas para configurar un nuevo sistema criptográfico disperso y distribuido, que es similar a otros tipos de redes en el sentido de que "no hay autoridad central alguna" ni forma universal alguna de usar el sistema criptográfico. Asimismo, no hay nada que se parezca a un registro público similar a la cadena de bloques - la RC es totalmente privada. Esta es completamente secreta y no hay peligro de capturar un mensaje y desencriptarlo más tarde con los ordenadores cuánticos futuros y demás. Existen numerosas cuestiones sutiles que aumentan la sofisticación de la implementación y amplían las aplicaciones más allá del intercambio simple de mensajes - banca, monedas electrónicas, VoIP, conversación, etc. Ello no es diferente a una red en malla con resonadores criptográficos en cada nodo. Cada nodo se puede conectar a cada uno de los otros nodos, que están transmitiendo por secuencias, continuamente, números pseudoaleatorios 24 horas al día, 7 días a la semana. Elegir una libreta de un solo uso en esta red es lo mismo que seleccionar un trayecto a través de todos o algunos de los nodos. Cada enlace añade más complejidad a la secuencia de encriptación ya que ninguna persona posee todos los nodos - estos son tolerantes a que cualquier número de nodos sean puestos en peligro por un enemigo que quiere sustraer información secreta encriptada por RC. Cualquier oyente clandestino mal intencionado aumentaría en realidad la seguridad del sistema al participar en él, lo cual es una característica potente.

Cuanto más largo sea el trayecto de un usuario de RC a través de esta web, más difícil será para alguien recrearlo y descifrar el secreto. Asimismo, el trayecto no es fijo - este cambia de segundo a segundo, por lo que un adversario necesitaría saber el nanosegundo exacto en el que un usuario se adentró en el trayecto. Además, tendrían que conocer el algoritmo que la aplicación de un usuario de RC está usando para encriptar mensajes usando este trayecto aleatorio. Asimismo, la mezcla de señales criptográficas, la temporización y otros factores aumenta de forma exponencial los recursos necesarios para descifrarlo. Este sistema tiene una propiedad importante en la criptografía que se puede expresar como "es computacionalmente fácil encriptar y desencriptar los mensajes en un grupo, pero para un extraño es inabordable realizar un ataque por fuerza bruta para hacer lo mismo". La grabación de cada señal no es práctica debido al gran volumen de almacenamiento de datos requerido - mucho más allá de la capacidad de almacenamiento conocida de todos los ordenadores en el mundo en la actualidad. Asimismo, el aumento geométrico en el número de permutaciones de estas señales para recrear una sola OTP es prohibitivo. Con un pequeño número de resonadores criptográficos, el número de combinaciones superaría rápidamente el número de partículas en el universo.

Otros ejemplos solucionan el problema de proximidad - los atacantes alejados no pueden sincronizar de forma simultánea sus vectores de ataque con el entorno dependiente del estado del usuario de RC. Esto significa que los atacantes están siempre en desventaja, ya que no pueden igualar el intercambio seguro entre los usuarios de RC - nunca pueden resonar en armonía con los usuarios dentro de este círculo criptográfico de confianza. Además, derrota los ataques de hombre en el medio ya que los usuarios de RC cuentan con secuencias paralelas de encriptación a través de muchos canales encriptados - el oyente clandestino ha de interceptar cada canal de forma simultánea para recrear un único mensaje y, entonces, desencriptarlo. No hay una clave criptográfica central para sustraer e irrumpir en el repositorio de secretos de una empresa. Solo hay un estado efímero de lucidez en el espacio criptográfico de RC accesible por usuarios privilegiados en cualquier momento en el tiempo. No hay una clave maestra para abrir cada uno de los archivos bloqueados. El cifrado no tiene lugar en bloques de datos, sino en una secuencia de números aleatorios con información incrustada de tamaño y escala arbitrarios, que fluye en una red.

En el modelo de RC, el tiempo de desplazamiento de las señales es importante ya que la luz atraviesa las redes de fibra óptica en torno a los encaminadores, centros de datos, etc., del mundo, para conectar a los usuarios finales con

los datos deseados - esta señal tiene un límite de velocidad fundamental y un tiempo de entrega dependiente de la infraestructura que atraviesa la misma. Dos usuarios pueden recibir información del mismo servidor en momentos ligeramente diferentes basándose en estos múltiples factores. Debido a que las claves criptográficas modernas son independientes del tiempo, cualquiera que las sustraiga puede desencriptar cada mensaje encriptado de la red de una empresa remontándose al principio del tiempo, o siempre y cuando las claves fueran válidas. La RC es completamente diferente - a menos que un atacante tenga una máquina del tiempo para capturar un comunicado y desencriptarlo en el futuro. Cualquier sistema en un estado resonante sería fundamentalmente difícil de piratear ya que un pirata informático tendría que estar físicamente casi encima de la víctima potencial, o el tiempo de desplazamiento para las señales sería diferente y, por lo tanto, no resonante - este solo ve datos encriptados a menos que pueda igualar completamente, momento a momento, el comportamiento del usuario de RC. La resonancia temporal con la que puede contar un pirata informático se vuelve incoherente con el tiempo y el espacio a medida que se establece el túnel seguro entre comunicadores de confianza - el pirata informático se queda sordo casi de inmediato, incluso si tiene un acceso excelente a las partes de una red.

Ninguna combinación de software / hardware se puede asegurar y comunicarse con el mundo exterior de manera significativa. La vulnerabilidad aumenta con la complejidad, mientras que RC sirve como contrapeso - este reduce la superficie de ataque global del sistema disponible para un pirata informático externo. Esto también vuelve tecnológicamente prohibitivas las mediciones criptográficas de un sistema. Por ejemplo, ¿puede un pirata informático o un atacante a nivel estatal capturar datos suficientes para caracterizar y aprovechar completamente un sistema de RC? Sí, es teóricamente posible, pero los recursos necesarios para hacerlo serían inviables desde los puntos de vista económico y práctico. Asimismo, los beneficios solo serían temporales y no tendrían relevancia alguna en el futuro inmediato.

En algunos ejemplos, aunque algunos resonadores criptográficos son solo balizas de números aleatorios que difunden datos de forma pasiva - el usuario no necesita alertar al resonador de que se está usando la señal - otros son interactivos, como una conexión de VPN a un sitio web. Cada uno de tales acoplamientos se puede preparar de tal manera que perturbe el resonador para todos los que también estén acoplados al mismo. Esto tiene la propiedad de perturbar el sistema conectado y dejar saber a todos que se ha unido a la red - un pulso básicamente pasa por el estado normal de generación de números aleatorios para incluir información acerca del nuevo participante y la temporización de su llegada. Se puede añadir una firma única a la nueva secuencia de números aleatorios para reflejar los acoplamientos de este usuario a otros resonadores, lo que garantiza una participación armoniosa en las comunicaciones privadas. El intento de unirse de un intruso será reconocido inmediatamente y será, en la práctica, incapaz de conectarse.

La RC tiene fuertes implicaciones para la gestión de identidad y la banca móvil. Aunque se sabe, incluso en la actualidad, que son insuficientes uno o dos puntos de datos para la autenticación de múltiples factores, en el futuro serán esenciales un mínimo de cinco o más. Con cada nuevo punto de datos, el problema del impostor se vuelve más difícil. La biometría ordinaria, como las huellas dactilares, no servirá por sí sola. Esta ya ha sido copiada, explorada y usada por delincuentes en paneles táctiles de iPhone y sensores relacionados. Una biometría más fuerte requiere que los usuarios consientan unas exploraciones faciales sumamente molestas y, probablemente algún día, el propio ADN. Esto será tanto ofensivo como inaceptable para la mayoría de los estadounidenses - la idea de ser rastreado como en la película Minority Report. Sin embargo, casi todos son felices portando y llevando puestos dispositivos electrónicos que usan aplicaciones que son recolectores de macrodatos sobre los individuos que los usan. La diferencia es que una persona puede optar por abandonar o participar en la mayor parte de las recopilaciones y siempre tiene la falsa sensación de seguridad de que puede elegir permanecer anónima.

Cualquiera puede comprar, registrar y usar un teléfono inteligente, iPod, Fitbit, banda deportiva, etc., todo ello bajo seudónimo y nunca permitir que estas empresas tengan información detallada acerca del usuario - consistiendo el temor en que esta se pueda usar contra el individuo para fines de seguro, admisiones universitarias, etc., y otras preocupaciones de privacidad. Con la RC, se puede realizar una autenticación no biométrica potente sin pérdida alguna de privacidad ni atribución alguna a la identidad verdadera de una persona - esto es importante para las monedas electrónicas y las transacciones en línea. Una persona es una "coincidencia" para una transacción si está de acuerdo una combinación de un número arbitrariamente grande de resonadores de RC públicos y privados. La decisión depende de la persona o institución - más acoplamientos conducen a más seguridad y conducen a un problema de pirateo informático más inabordable - esto incumbe al nivel de Punto de Venta en unos grandes almacenes. Además, cualquier pirateo es únicamente temporal, si es que alguna vez se descubre una técnica. Este es bueno solo para una transacción o sesión única - no es lo mismo que sustraer un número de tarjeta de crédito y credenciales de respaldo, ni conlleva el riesgo de que alguien sustraiga la biometría digitalizada de una persona - una persona no puede obtener una nueva cara o huellas dactilares para mitigar el daño. Con la RC, una persona simplemente comienza una nueva sesión y el pirata informático vuelve a la casilla de salida. Las capas de seguridad evolucionan mucho más rápido de lo que los piratas informáticos pueden piratearlas, ya que la complejidad no crece de forma lineal sino exponencial.

El almacenamiento de datos estáticos se puede encriptar de diversas maneras usando un sistema similar. Por ejemplo, algunos resonadores podrían transmitir una señal de repetición continua en una escala de tiempo arbitraria, dependiendo del nivel de seguridad requerido, desde nanosegundos a meses o años. Se podría generar una OTP

única a partir de esta señal como una combinación matemática de un registro público y / o privado del cual hay múltiples copias. La "clave" para replicar esta OTP a petición sin tener que almacenar una OTP masiva podría ser una función combinatoria de tiempo y señal simple para ese conjunto de datos. Debido al enorme número de funciones, en combinación con el número de secuencias de resonador, el número resultante de posibilidades de OTP es significativamente más difícil de adivinar que cualquier esquema de encriptación actual generado usando hardware informático avanzado.

Otros ejemplos más de RC incluyen la cascada de conexiones - perturbar rápidamente el sistema de resonadores con cada usuario nuevo hasta que solo se pueda establecer firmemente el círculo de confianza, y ningún tercero podría replicar el patrón. Esto permite que se formen redes de resonadores y que estas conspiren mutuamente para aumentar la aleatoriedad y la seguridad globales del propio sistema. Otro punto clave que recordar es que resulta fácil validar cada elemento de esta construcción. Las OTP son fáciles de entender y todos han experimentado, de una u otra forma, la resonancia.

Se puede usar texto de cifrado de relleno - secuencias de datos sin sentido - para contaminar el sistema sin coste informático alguno para los usuarios validados. Esto aumenta adicionalmente los recursos informáticos necesarios para atacar la red de resonadores y se puede usar para ofuscar la temporización de los mensajes - los usuarios están difundiendo continuamente, pero solo una minoría de la transmisión es texto de cifrado real.

Las soluciones complejas específicas del cliente - la personalización del algoritmo de RC para un cliente - es una cuestión de cálculo de la ventaja matemática de cualquier ecuación. Esto es equivalente a darle al cliente un paladar aceptable sobre el cual construir su propia solución criptográfica usando las redes y principios centrales de RC.

Los ejemplos simples de aplicaciones pueden incluir un cifrado de secuencia de OTP continuo usado para encriptar y controlar el acceso por abono a cualquier red de entrega de contenido (CDN) o secuencia en vivo de cualquier tipo de datos. Aunque se podría usar un número de puntos de RC públicos para la encriptación en masa, se podría usar un único punto de RC de control para administrar el acceso de los usuarios ya que cualquier elemento de la alimentación de RC podría cortar el servicio a destinatarios no autorizados. Esto es análogo a difundir ampliamente los datos encriptados por el aire sin riesgo de que nadie salvo usuarios previstos obtenga acceso - esto también es de aplicación a la jerarquía del modelo de acceso en donde la misma secuencia encriptada en masa podría permitir unos niveles variables de uso y desencriptación. Por ejemplo, un proveedor puede querer dar a los clientes de pago escalonado más contenido para servicios o contenido de pago al tiempo que se sigue ofreciendo de manera segura el producto esencial a los usuarios que no son de pago.

Otros ejemplos de encriptación de igual a igual pueden permitir a los usuarios enviarse entre sí paquetes encriptados pequeños, tales como identidades con hash con una clave de sesión aleatoria o fija. Este anexo pequeño puede crear una secuencia única a partir de un resonador único, o de una combinación de resonadores, al alterarlos de manera significativa, tal como añadir un múltiplo trascendente, permutación, eliminación y otros cálculos de uso poco intensivo de CPU.

Por lo tanto, debido a que la Transmisión Criptográfica por Secuencias permite que cualquier resonador proporcione una secuencia criptográfica en vivo para realizar una transición de flujos de información y conectividad estática a dinámica basada en el tiempo, los ejemplos anteriores y posteriores se vuelven útiles para encriptar secuencias de datos perpetuas en tiempo real en lugar de realizar operaciones criptográficas sobre datos en reposo en una única ubicación física o en la nube. En este sentido, los datos en vivo se transforman en información encriptada de transmisión por secuencias.

A medida que la naturaleza de la computación evoluciona hacia un modelo siempre activo de canalizaciones de información, la RC se convertirá en el ingrediente esencial para asegurar la próxima evolución de Internet y de las redes posteriormente a IP. Este estado siempre activo es muy diferente de los que existen en la actualidad, principalmente ya que no implicará necesariamente la participación activa de los usuarios finales. De acuerdo con los requisitos de los dispositivos o usuarios de punto de extremo, la información fluirá según sea necesario o prescrito por los usuarios o propietarios de los sistemas, de manera no diferente a una fuente de noticias continua basándose en las preferencias de contenido de usuario. Aunque Internet está siempre activo en la actualidad en el sentido de que las redes globales están en funcionamiento continuo, el siguiente estado siempre activo será mucho más dinámico, con unos volúmenes de información mucho mayores que se moverán de forma autónoma por diseño. El aprendizaje automático reemplazará la toma de decisiones humanas sobre el tráfico de información y creará un modelo de utilización más eficiente y refinado.

A medida que el Internet de las cosas (IoT) emerge a una red de sensores universal que responde directamente a los cambios en el entorno tecnológico al que da servicio, el movimiento seguro de los datos de sensor para proteger frente a la corrupción o manipulación de datos requiere una capa más fundamental de seguridad, integrada en la transmisión por secuencias de la información en sí misma. El acoplamiento de RC pasivo o activo a estos dispositivos crea un marco criptográfico sólido para ofuscar los datos y las relaciones entre varias secuencias de datos. Esto es importante para evitar el análisis de tráfico de información, la caracterización y, en última instancia, el pirateo informático. Las redes de RC en capas que usan técnicas de transmisión criptográfica por secuencias a

través de cualquier red de sensores complican en gran medida la tarea de irrumpir en la red y estudiar su comportamiento. Por lo tanto, su seguridad es fuerte y no existe ni un solo punto de fallo o ataque, lo cual es un nuevo paradigma muy alejado de los sistemas actuales.

Por ejemplo, una única puesta en peligro de un almacén de claves o servidor criptográfico centralizado puede permitir a un atacante una visibilidad total en la red a la que da servicio, incluyendo la capacidad de desencriptar cualquier paquete transmitido o recibido desde fuera del sistema. En el modelo de RC, esta vulnerabilidad se supera distribuyendo hacia delante y diversificando el material criptográfico usado para asegurar un sistema. Incluso si todas las partes de este modelo son bien entendidas, capturadas y puestas en peligro por un atacante, las comunicaciones seguras entre los usuarios se siguen logrando fácilmente y pueden seguir siendo consideradas seguras frente a una escucha clandestina por otros atacantes que no estén al tanto del material puesto en peligro. En este sentido, el modelo de RC es sumamente resistente y más seguro más allá de la alta resistencia demostrable de las OTP. Los usuarios de punto de extremo que deseen comunicarse directamente pueden tener protocolos de implementación de encriptación privados y únicos que usan una red de RC puesta en peligro.

Un resonador puede incluir un generador de números aleatorios. El RNG puede incluir al menos uno de un generador de números aleatorios verdaderos, un generador de números pseudoaleatorios o cualquier secuencia no repetitiva de números que tenga una característica de una secuencia de números aleatorios. Como anteriormente, el generador de números aleatorios puede generar una primera secuencia de números aleatorios. El resonador puede incluir un transmisor que se puede acoplar eléctricamente al generador de números aleatorios. El transmisor transmite la primera secuencia de números aleatorios al menos por radiofrecuencia o a través de una red. El resonador también puede incluir un receptor para recibir secuencias de números a partir de otros dispositivos analizados a continuación. Un experto en la materia entiende fácilmente que el transmisor y el receptor pueden ser, en algunos ejemplos, uno en el mismo elemento, un transceptor. Este incluye cualquier procesamiento requerido para o bien enviar o bien recibir las secuencias.

También se puede incluir un procesador que integra una segunda secuencia de números en la primera secuencia de números aleatorios para formar una secuencia combinada y una memoria de resonador no transitoria para almacenar datos. La segunda secuencia de números se puede recibir desde un segundo resonador u otro dispositivo de usuario analizado a continuación.

Se puede usar un comunicador para comunicarse con el resonador y otros dispositivos de usuario. Las comunicaciones en el contexto de la presente invención incluyen recibir secuencias de números aleatorios a partir de uno o más resonadores, transmitir números de comunicador al resonador y comunicarse con otros comunicadores para intercambiar texto sin formato y comunicaciones encriptadas y el algoritmo para generar una clave de encriptación.

Para facilitar estas capacidades, el comunicador tiene un receptor de comunicador que puede recibir la primera secuencia, así como un motor criptográfico de comunicador que se puede enlazar electrónicamente al receptor de comunicación. El motor criptográfico también puede incluir una memoria no transitoria y un procesador enlazado electrónicamente a la memoria. Un ejemplo de las tareas del motor criptográfico de comunicador puede ser leer al menos una porción de la primera secuencia y convertir la porción de la primera secuencia en una clave criptográfica.

En ejemplos adicionales, puede haber un segundo o más comunicadores como parte del sistema, estos comunicadores adicionales pueden tener más o menos capacidades que el comunicador descrito anteriormente. Cuando el primer comunicador se comunica con el segundo, por ejemplo, cuando Alice se comunica con Bob, como se describe en los muchos ejemplos anteriores, el primer y el segundo procesadores de comunicador tienen un algoritmo común para convertir independientemente la porción de la primera secuencia en la clave criptográfica. Esta es una de las ventajas de la invención, ni Alice ni Bob tienen que compartir una clave, cada uno genera la suya de forma independiente. Esta clave también se genera solo en el momento en el que se necesita, por lo que no está almacenada, esperando para desbloquear datos en el futuro. Esto aumenta la seguridad ya que, al no ser necesario transmitir la clave, esta no puede ser interceptada. Asimismo, dado que se genera sobre la marcha para cada conjunto de datos, la posesión de una clave antigua no permite la desencriptación de ningún dato futuro o dato pasado distinto de los datos para los que se generó la clave.

Para incluir algo de hardware en los ejemplos anteriores, como ya se ha indicado, el receptor de comunicador puede recibir una segunda secuencia de números desde un segundo resonador. La memoria no transitoria puede almacenar al menos una porción de la segunda secuencia. El procesador de comunicador puede leer entonces la porción de la segunda secuencia y usa ambas porciones, para crear la clave criptográfica.

Otros ejemplos hacen que el comunicador también incluya un generador de números de comunicador que pueda generar un número de comunicador. El generador de números de comunicador puede ser un RNG como se ha descrito anteriormente para generar secuencias aleatorias o pseudoaleatorias a insertar en la secuencia de un resonador. El generador de números de comunicador también puede generar secuencias no aleatorias que se pueden usar para identificar el comunicador o, en coordinación con el motor criptográfico, para insertar mensajes, como se describe a continuación.

El comunicador también puede incluir un transmisor de comunicador que transmite el número de comunicador al resonador. El receptor de resonador recibe el número de comunicador; y el procesador de resonador puede integrar el número de comunicador en la secuencia de números aleatorios para formar una secuencia combinada que puede ser transmitida por el transmisor.

En otros ejemplos indicados anteriormente, una vez que el número de comunicador se inserta en una secuencia de resonador combinada, un segundo comunicador puede recibir la secuencia combinada y detectar el número de comunicador. Una vez así informado, el segundo comunicador puede generar su propio (un segundo) número de comunicador. El primer y el segundo números de comunicador se pueden enviar entonces al resonador para combinarse con la secuencia de resonador para hacer una segunda secuencia combinada que pueda ser transmitida por el transmisor.

Aún otros ejemplos de RC involucraron la temporización de las secuencias. Así, el transmisor de resonador puede transmitir una porción de la primera secuencia en un instante T0. Esta primera secuencia de T0 puede ser grabada, ya sea por un segundo dispositivo (como un comunicador) o por el propio resonador. Independientemente de qué dispositivo la grabe, la primera secuencia de T0 se puede almacenar en la memoria del resonador (es decir, ya estaba allí si fue grabada por el resonador, o se puede recibir de vuelta a través del receptor cuando se grabara en otro lugar). El procesador puede combinar entonces la primera secuencia de T0 con una porción de la primera secuencia en un instante T1 para formar una secuencia recursiva que se transmite entonces.

Otros ejemplos que usan la temporización de las secuencias incluyen un conjunto de datos 302 que tiene al menos un valor VI. En el presente caso, el resonador transmite una porción de la primera secuencia en un instante T0 y el motor criptográfico de comunicador puede encriptar el valor VI usando la primera secuencia de T0. El resonador también puede transmitir una porción de la primera secuencia en un instante T1. Esto puede permitir que el motor criptográfico de comunicador descifre el valor V1 usando la primera secuencia de T0 y vuelva a cifrar el valor V1 usando la primera secuencia de T1. La criptografía de ámbar, como se ha indicado anteriormente, es otro ejemplo de uso de un segmento de tiempo de una secuencia. Una memoria no transitoria de ámbar puede almacenar la primera secuencia de T0 y un conjunto de datos se puede encriptar usando la primera secuencia de T0.

Más ejemplos del uso de múltiples resonadores y / o múltiples comunicadores pueden dar como resultado la secuencia recombinante descrita anteriormente. En el presente caso, el segundo resonador transmite una segunda secuencia de números y el comunicador puede recibir la primera y la segunda secuencias. El motor criptográfico de comunicador puede combinar la primera y la segunda secuencias para formar la secuencia recombinante que puede ser transmitida por el primer transmisor de comunicador. La secuencia recombinante se puede formar habitualmente cuando el primer motor criptográfico de comunicador aplica un algoritmo, en un ejemplo Frc(n), a la primera y la segunda secuencias, para formar la secuencia recombinante.

Otros ejemplos pueden dar como resultado comunicaciones "fantasma". En el presente caso, el primer número de comunicador puede ser un mensaje en texto claro transmitido al resonador usando una primera secuencia para formar la "secuencia fantasma" combinada de la primera secuencia y la primera secuencia del primer número de comunicador. Entonces, un segundo comunicador puede recibir la secuencia fantasma y su motor criptográfico aplica el filtro que filtra el primer número de comunicador de la secuencia fantasma. Obsérvese que se puede usar cualquier número de resonadores y sus secuencias para dividir entre ellos el mensaje.

También se pueden analizar los ejemplos de vallas geográficas. En el presente caso, el transmisor de resonador es un transmisor de corto alcance y un alcance de señal de transmisor define un área de valla geográfica. Cuando el receptor de comunicador recibe la primera secuencia de números dentro del área de valla geográfica, el motor criptográfico de comunicador puede crear la clave criptográfica necesaria para acceder a cualesquiera conjuntos de datos o hardware que sean parte del área de valla geográfica. A la inversa, cuando el comunicador está fuera del área de valla geográfica, por ejemplo, ya no puede recibir la señal de transmisor, el motor criptográfico de comunicador no puede crear la clave criptográfica. Esto se puede observar fácilmente, ya que si un usuario no puede acceder al resonador adecuado, nunca tendrá toda la información necesaria para leer la información encriptada.

Los siguientes ejemplos describen los métodos de uso de RC en etapas. Obsérvese que estas etapas pueden ser realizadas por el hardware analizado en el presente documento y se pueden materializar en hardware especialmente diseñado o en software que se ejecuta en hardware habitual o patentado.

Un ejemplo de un método para encriptar y desencriptar datos usando criptografía resonante, estas son las etapas básicas del resonador, que incluyen generar una primera secuencia de números aleatorios usando el resonador y, entonces, transmitir la primera secuencia de números usando un transmisor. La figura incluye adicionalmente el método de enmarañamiento básico, que puede incluir las etapas de recibir, en el resonador, la segunda secuencia de números. La primera secuencia y la segunda secuencia se pueden combinar, usando un procesador en el resonador, para formar una secuencia combinada y, entonces, transmitir la secuencia combinada con el transmisor.

Algunos de los ejemplos que involucran al comunicador incluyen recibir la primera secuencia en un comunicador y, entonces, almacenar al menos una porción de la primera secuencia en la memoria del comunicador. El procesador del comunicador puede convertir la porción de la primera secuencia en una clave criptográfica. Esto se puede hacer usando un algoritmo.

Añadir al menos un comunicador más permite que dos partes se comuniquen de manera segura. Este método hace que el segundo comunicador reciba la primera secuencia y almacene una porción de la misma. El segundo comunicador puede convertir la porción de la primera secuencia en la misma clave criptográfica usando el mismo algoritmo. Como anteriormente, esto permite que Alice y Bob se comuniquen usando la misma clave, pero generada de forma independiente y, en algunos ejemplos, sobre la marcha.

Un ejemplo del uso de múltiples resonadores permite que el comunicador reciba la segunda secuencia de números generada por un segundo resonador y almacene al menos una porción de la misma. Las porciones de la primera y la segunda secuencias se pueden convertir en una clave criptográfica usando un algoritmo.

La combinación de secuencias de resonador y de comunicador es un ejemplo de un método de convergencia. Este ejemplo hace que el resonador reciba el número de comunicador, generado por el primer comunicador. Esta etapa se toma desde el punto de vista del resonador, pero en otros ejemplos puede ser fácilmente el caso que el comunicador generara el número de comunicador y lo transmitiera al resonador. Sin embargo, puede ser que el resonador combine el número de comunicador, con la primera secuencia en una secuencia combinada y, entonces, la transmita.

Continuando con el ejemplo anterior, esta secuencia combinada permite a Alice señalizar (o más) a Bob en secreto. Este método incluye recibir, en un segundo comunicador, la secuencia combinada y, entonces, almacenar al menos una porción de la misma. El procesador del segundo comunicador puede detectar la porción del número de comunicador, a partir de la secuencia combinada.

Un ejemplo de un método de conexión en cascada incluye en donde el resonador recibe (o recibe de vuelta) un segundo número de comunicador generado por el segundo comunicador y el primer número de comunicador, ambos transmitidos por el segundo comunicador. El resonador combina el primer y el segundo números de comunicador con la primera secuencia en una segunda secuencia combinada y, entonces, la transmite.

Además, un método para formar la secuencia recombinante es en donde el primer comunicador recibe entonces la primera secuencia y la segunda secuencia de números (habitualmente generada por un segundo resonador). Las dos secuencias se alteran y / o se combinan usando alguna forma de algoritmo para convertir así una porción de la primera y la segunda secuencias en la secuencia recombinante. La secuencia recombinante se transmite con un primer transmisor de comunicador.

Ejemplos en los que se toman segmentos de la secuencia en momentos diferentes para obtener resultados criptográficos más avanzados. Para una secuencia recursiva, un ejemplo de un método incluye generar una primera secuencia de números aleatorios en un instante T0 usando el resonador. Una porción de la primera secuencia de T0 se almacena en una memoria no transitoria. Este almacenamiento puede ser en el mismo resonador que generó la primera secuencia de T0, un resonador diferente o un comunicador. Independientemente de dónde se almacene, la primera secuencia de T0 se envía de vuelta al resonador para combinarse con una porción de la primera secuencia en un instante T1 para formar una secuencia recursiva que se transmite entonces.

Otro método de segmentos de tiempo, ilustrado en una figura, permite que valores separados disponibles públicamente se encripten con el tiempo. En este método, el comunicador recibe la primera secuencia de T0 y encripta un primer valor de datos V1 usando la primera secuencia de T0. Separada en el tiempo, entonces el comunicador recibe del resonador una primera secuencia de T1. El valor de datos V1 se puede desencriptar entonces usando la primera secuencia de T0 y encriptarse entonces usando la primera secuencia de T1.

Un ejemplo de tiempo más es la criptografía de ámbar. En el presente caso, un ejemplo de un método incluye generar una primera secuencia de números aleatorios en un instante T0 usando el resonador (como anteriormente). La primera secuencia de T0 se almacena en una memoria de ámbar y se usa para encriptar un conjunto de datos. Sin embargo, una vez encriptado de esta manera, no hay forma de que un actor malo escuche en busca de la secuencia de T0, se pierde en el tiempo.

La RC fantasma puede ser otra herramienta potente. Esta se puede usar para enviar texto claro en secuencias públicas, Bob solo necesita saber qué secuencias y qué segmentos son segmentos fantasma a partir del segmento público de las secuencias. Esta también puede enviar un mensaje encriptado para acrecentar su enturbiamiento. Un ejemplo de este método puede ser al generar, en el primer comunicador, un primer número de comunicador que es un mensaje en texto claro. El primer número de comunicador se puede transmitir al resonador usando una primera secuencia. El primer número de comunicador se combina con la primera secuencia para dar una secuencia fantasma en el resonador. El segundo comunicador recibe la secuencia fantasma y la filtra para extraer el primer número de comunicador de la secuencia fantasma.

Otro ejemplo puede conducir a un método de vallado geográfico de un área para restringir el acceso a datos. Un ejemplo, ilustrado en una figura, define el área vallada geográficamente basándose en el alcance de señal del transmisor que transmite la primera secuencia. Una vez definida, se puede permitir o denegar el acceso a los datos de vallador geográfico basándose en la recepción de la primera secuencia en el primer comunicador. Si se recibe la primera secuencia, se puede crear la clave criptográfica usada para desencriptar los datos en el área vallada geográficamente.

Breve descripción de los dibujos

Los aspectos anteriores y aspectos adicionales de la presente invención se analizan adicionalmente con referencia a la siguiente descripción junto con los dibujos adjuntos, en los que números semejantes indican características y elementos estructurales semejantes en diversas figuras. Los dibujos no están necesariamente a escala, resaltándose en su lugar la ilustración de los principios de la invención. Las figuras representan una o más implementaciones de los dispositivos de la invención, solo a modo de ejemplo, no a modo de limitación.

la figura 1 es un ejemplo de una red de resonadores criptográficos de la presente invención;
la figura 2 es un diagrama que ilustra un intercambio criptográfico resonante básico entre Alice y Bob;
la figura 3 es un diagrama que ilustra un intercambio criptográfico resonante básico más complejo entre Alice y Bob;
la figura 4 es un diagrama que ilustra una formación criptográfica resonante acoplada de una secuencia derivada;
la figura 5 es un diagrama que ilustra un ejemplo de intercambio criptográfico resonante acoplado entre Alice y Bob;
la figura 6 es un diagrama que ilustra otro ejemplo de una formación criptográfica resonante acoplada de una secuencia derivada;
la figura 7 es un diagrama que ilustra un ejemplo de llamada de la presente invención;
la figura 8 es un diagrama que ilustra un ejemplo de conexión en cascada de la presente invención;
la figura 9 es un diagrama que ilustra un ejemplo de criptografía recursiva de la presente invención;
la figura 10 es un diagrama que ilustra un ejemplo de criptografía recombinante de la presente invención;
la figura 11 es un diagrama que ilustra un ejemplo de criptografía de viaje en el tiempo de la presente invención;
las figuras 12A y 12B son diagramas que ilustran ejemplos criptográficos fantasma de la presente invención;
la figura 13 es un diagrama que ilustra un ejemplo de punto de control criptográfico de la presente invención;
la figura 14 es un diagrama que ilustra un ejemplo criptográfico de ámbar de la presente invención;
la figura 15 ilustra un ejemplo de un resonador de la presente invención;
la figura 16 ilustra un diagrama de un comunicador de la presente invención;
la figura 17 es un diagrama de flujo que ilustra un ejemplo de un método de resonador de la presente invención;
la figura 18 es un diagrama de flujo que ilustra un ejemplo de un método de comunicador de la presente invención;
la figura 19 es un diagrama de flujo que ilustra un ejemplo de un método de convergencia de la presente invención;
la figura 20 es un diagrama de flujo que ilustra un ejemplo de un método de señalización de la presente invención;
la figura 21 es un diagrama de flujo que ilustra un ejemplo de un método de secuencia combinada de la presente invención;
la figura 22 es un diagrama de flujo que ilustra un ejemplo de un método de secuencia recombinante de la presente invención;
la figura 23 es un diagrama de flujo que ilustra un ejemplo de un método de secuencia recursiva de la presente invención;
la figura 24 es un diagrama de flujo que ilustra un ejemplo de un método de encriptación de datos públicos de la presente invención;
la figura 25 es un diagrama de flujo que ilustra un ejemplo de un método de almacenamiento de ámbar de la presente invención;
la figura 26 es un diagrama de flujo que ilustra un ejemplo de un método de comunicación fantasma de la presente invención; y
la figura 27 es un diagrama de flujo que ilustra un ejemplo de un método de vallado geográfico de la presente invención.

Descripción detallada

La criptografía de resonancia ("RC") es un método de encriptación segura que imita, a lo que puede ser una escala global, el método de encriptación de Libreta de un Solo Uso ("OTP") que (cuando se implementa correctamente) es impenetrable. El método, y los dispositivos que lo implementan, crean y utilizan un entorno de uno o más resonadores criptográficos 100 para difundir una secuencia 102 de números de apariencia aleatoria. Un ejemplo simple de un resonador criptográfico 100 es un generador de números aleatorios ("RNG"). El resonador criptográfico / RNG 100 puede ser un generador de números aleatorios verdaderos, un generador de números pseudoaleatorios o cualquier secuencia no repetitiva de números con la apariencia y características de una secuencia de números

aleatorios. El resonador criptográfico 100 se puede implementar en uno o más de hardware o software y generarse y / o transmitirse mediante técnicas digitales o analógicas.

La figura 1 ilustra algunos ejemplos de los resonadores criptográficos 100. Una baliza de resonador criptográfico simple 100A es similar a un punto de acceso inalámbrico y genera una secuencia verdaderamente aleatoria de dígitos 102A. La baliza 100A es una radiodifusión pública y es accesible por cualquier usuario 200A dentro del alcance de la señal 102A. Una radio de resonador criptográfico 100B puede generar su secuencia 102B por software y proyectarla a través de una red 300 a cualquier usuario 200B con acceso a esa red 300. En este ejemplo, la secuencia 102B de la radio de resonador criptográfico 100B puede ser pseudoaleatoria. La red 300 puede ser tan expansiva como Internet o tan restrictiva como una red de área local ("LAN") de una empresa. Otro tipo de resonador criptográfico 100 es un resonador criptográfico seguro 100C. El resonador criptográfico seguro 100C puede permitir el acceso solo a usuarios 200C que son miembros (por ejemplo, empleados de una empresa) o abonados que pagan por la secuencia privada 102C. En este ejemplo, la secuencia privada 102C es una secuencia no repetitiva (por ejemplo, pi o e). Obsérvese que cualquiera de los resonadores criptográficos 100A, 100B, 100C puede generar cualquier tipo de secuencia: aleatoria, pseudoaleatoria o no repetitiva, y cualquier usuario 200A, 200B, 200C puede tener acceso a algunas o todas las secuencias 102A, 102B, 102C.

Los ejemplos de la configuración anterior se pueden conocer como una Red Criptográfica Resonante. Para cualquier red de dispositivos informáticos que se comuniquen de forma segura, la RC es una red en malla de unos resonadores 100 que transmiten secuencias de unos datos 102 a los receptores de encriptación 103 (por ejemplo, cualquier almacenamiento o dispositivo de usuario indicado en los ejemplos a continuación) para generar una OTP efectiva de formas complejas. Esto se puede lograr mediante cualquier número de algoritmos, tanto estáticos como dinámicos, para encriptar datos de forma tanto pública como privada para usuarios fiables. También se puede usar para cualquier medio seguro de ofuscar datos más allá de una encriptación simple. Si se usa como un cifrado de clave simétrica, la longitud de la clave no es fija y puede crecer de forma arbitraria con el ancho de banda de los resonadores 100 o la red de resonadores 100. Además, las mismas secuencias pueden ser usadas por un número ilimitado de usuarios 200 que varían, todos ellos, su implementación, incluyendo la encriptación de secuencias.

Cada secuencia 102 puede actuar como su propia OTP para cualquier usuario 200 que pueda acceder a esa secuencia 102. La secuencia 102 puede ser una clave de cifrado real 104 o la base matemática para la clave de cifrado 104. Una vez que dos usuarios 200 acuerdan uno o más resonadores criptográficos 100, y cuando comienzan a acceder a la secuencia 102 para crear la clave, el cifrado se puede crear sobre la marcha y no se puede duplicar ni vulnerar.

Un ejemplo muy simple es que un primer usuario, Alice 202A, quiere encriptar un mensaje para un segundo usuario, Bob 202B. A partir de la figura 2, Alice 202A y Bob 202B acuerdan usar la baliza de resonador criptográfico 100A e introducir la secuencia 102A en un instante T1. Por lo tanto, tanto Alice 202A como Bob 202B comienzan a recopilar números aleatorios de entre la secuencia 102A (1971693993...). Alice y Bob 202A, 202B también han acordado usar un cifrado aditivo simple. El mensaje es "Hola", el cual, cuando se convierte en números por posición en el alfabeto, es 8-4-12-12-15. Los primeros 5 dígitos de la secuencia 102A tomados en el instante T1, que son 1-9-7-1-6, se convierten en la clave 104. Sumando los dos conjuntos de dígitos se obtiene el mensaje encriptado 106, que es 9-13-19-13-21, o 913191321. Bob 202B, después de haber capturado su propia versión de la clave 104 a partir de la secuencia 102A, puede descodificar entonces el mensaje al restar cada uno de los dígitos de la clave de cada uno de los dígitos de "letra" para recuperar el mensaje claro "hola".

Obsérvense algunas características clave de la invención, Alice y Bob 202A, 202B no tuvieron que intercambiar claves por adelantado, solo acordar cómo generar la clave. Además, ni Alice ni Bob 202A, 202B sabían cuál iba a ser la clave exacta hasta el instante en el que introdujeron la secuencia 102A. Si hubieran acordado introducir la secuencia 102A en un momento posterior, por ejemplo en el instante T1', la clave habría cambiado en unos pocos dígitos y hubiera sido 9-3-9-9-3. Por lo tanto, a pesar de que la baliza 100A está transmitiendo por secuencias 102A al público, no hay forma de que alguien sepa cuándo comenzar a usar la secuencia 102A para descifrar el mensaje. La clave, por supuesto, se puede hacer aún más compleja al realizar más que únicamente una adición simple para el algoritmo de encriptación.

La figura 2 también ilustra un esquema de encriptación ligeramente más complejo para Alice y Bob 202A, 202B. Para una seguridad más robusta, Alice y Bob 202A, 202B acuerdan usar también la radio de resonador criptográfico 100B y su secuencia 102B. También entran en la secuencia de radio 102B en el instante T1 y obtienen 4-1-0-2-7. Entonces, se acuerda que la suma de la secuencia de baliza 102A y la secuencia de radio 102B es la clave, por lo tanto 5-10-7-3-13, y el mensaje se encripta como se ha indicado anteriormente. Entonces, se pueden usar cada vez más secuencias para hacer que la clave sea cada vez más compleja, aunque ambas secuencias 102A, 102B son públicas. Se puede obtener aún más seguridad si Alice y Bob 202A, 202B usaran el resonador criptográfico seguro 100C y la secuencia privada 102C.

La figura 3 es otro ejemplo más con algo de complejidad. Hay una serie de balizas de resonador criptográfico 100A-1, 100A-2, 100A-3... 100A-X y una serie de resonadores criptográficos seguros 100C, que pueden ser privados o controlados por pertenencia / abono. Alice y Bob 202A, 202B desean enviar un mensaje seguro "1111" en un

momento determinado (por ejemplo, 01:00 UTC). Alice y Bob 202A, 202B acuerdan adicionalmente usar la baliza pública RC n.º 1 100A-1 y la RC n.º 314 100A-3 y un resonador seguro NCOIEWUH 100C-1. A las 01:00 UTC, las secuencias de cada uno de esos resonadores criptográficos 102A-1, 102A-3 y 102C-1 transmiten los siguientes cuatro dígitos de una serie de números aleatorios, 0200, 1234, 9876, respectivamente. Alice y Bob 202A, 202B acuerdan generar la clave por adición falsa (es decir, no importa lo que sumen los dígitos, solo se usa el dígito en la columna "unos"). Por lo tanto, la clave 104 es 1200. Alice y Bob 202A, 202B acuerdan nuevamente una adición falsa para encriptar el mensaje, que se convierte en el mensaje encriptado 106 "2311". Entonces, Alice 202A transmite el mensaje encriptado 106 en claro a Bob 202B, que ya tiene la clave 104, y desencripta el mensaje en consecuencia.

Algunos de los aspectos de la presente invención son evidentes simplemente a partir del ejemplo simple anterior. Incluso si el resonador seguro NCOIEWUH 100C-1 registra su secuencia completa con el tiempo, no hay forma de que un pirata informático sepa que Alice y Bob 202A, 202B acordaron usar también la RC n.º 1 100A-1 y la RC n.º 314 100A-3. Incluso si el pirata informático sabe exactamente cuáles son los resonadores, sigue sin saber cuándo decidieron introducir las secuencias 102A-1, 102A-3 y 102C-1 para comenzar la generación de la clave. Entonces, incluso con un conocimiento perfecto de los resonadores y el tiempo de entrada en las secuencias, el pirata informático sigue sin saber el algoritmo de encriptación.

En circunstancias normales, con solo unos pocos resonadores 100 en funcionamiento, existe una posibilidad casi nula de que un pirata informático pueda adivinar la clave 104. El pirata informático necesitaría haber grabado cada resonador 100 posible e intentar cada combinación y cada punto de entrada de tiempo (y eso es incluso con la suposición de que cada secuencia se introduce en el mismo punto en el tiempo). Incluso usando el más simple de los algoritmos de encriptación, este es un sistema mucho más robusto que el que está actualmente en uso, y proporciona una encriptación casi perfecta, con una clave muy ligera. En este ejemplo, la longitud de la clave es solo la longitud del mensaje encriptado 106. Además, la captura de las secuencias 102 y el algoritmo de encriptación simple se calcula fácilmente usando incluso los recursos limitados de la CPU de un dispositivo móvil.

Otro ejemplo, como se ilustra en las figuras 4 y 5, añade aún más complejidad y seguridad a la presente invención. En los ejemplos anteriores, los resonadores 100 pueden ser dispositivos pasivos, que simplemente emiten su secuencia 102. Un ejemplo de Enmarañamiento Criptográfico (CE) les permite volverse dinámicos y sensibles a su entorno. El CE es la propiedad de cualquier resonador 100 que permite que el resonador se acople a otros resonadores. Los ejemplos incluyen una secuencia pequeña, única para cualquier usuario 200 de la RC, generada por su generador / resonador de usuario personal 206 como un teléfono inteligente. Los ejemplos del acoplamiento pueden ser tan simples como el hash de dispositivo combinado con una firma de tiempo. En un ejemplo, el acoplamiento puede tener lugar siempre que no sea una secuencia estática de números. El usuario 200 del resonador 100 o cualquier combinación de los mismos en una red de RC puede quedar entonces enmarañado con el tiempo, al cambiar sus secuencias individuales en respuesta a aquellas con las que se acopla. Cada elemento de esta disposición evoluciona rápidamente con el tiempo para crear un nuevo estado criptográfico en donde cualquier característica única del sistema aislado se transforma de manera única. Las secuencias combinadas se enmarañan entonces entre sí estableciendo un sistema nuevo y complejo.

El enmarañamiento complica el problema de atacar la red, ya que cada nuevo elemento que se acopla al sistema cerrado de comunicadores es detectable. La modificación de la superficie criptográfica en uso alertará a cada elemento del sistema de forma simultánea. Esta es una capa secundaria de seguridad y detección de intrusiones que evoluciona a partir de esta forma usando una red de RC.

La figura 4 ilustra un ejemplo simple del usuario 200 interaccionando con el resonador 100. De esta manera, el usuario 200 puede difundir, desde un generador / resonador de usuario 206, una secuencia de usuario 204 para su inserción en una secuencia de resonador 102. Para un observador no informado, la adición de la secuencia de usuario 204 no se detecta, ya que sigue pareciendo que se están generando números aleatorios, pero para un usuario informado, esto se puede usar para mejorar la seguridad o como un identificador una vez que se ha detectado la secuencia de usuario 204 en la secuencia de resonador 102.

La inserción de la secuencia de usuario 204 en la secuencia de resonador 102 puede dar como resultado cualquier número de acciones diferentes. En el ejemplo simplificado de la figura 4, la secuencia de resonador 102 es solo "1s" y la secuencia de usuario 204 es solo "2s". La secuencia secundaria 208 resultante puede ser una función de alternar la secuencia de usuario 204 y la secuencia de resonador 102, dando como resultado un patrón de "121212121212". Como alternativa, esta puede ser una inclusión aditiva, dando como resultado entonces una secuencia secundaria 208 de "3333333333". Se puede realizar cualquier otra operación matemática en las dos secuencias 102, 204 para conducir a la secuencia secundaria 208 resultante.

La figura 5 ilustra un ejemplo de CE más complejo. En el presente caso, no solo el resonador de usuario 206 se puede acoplar con el resonador 100, sino que el resonador 100 se puede acoplar con el resonador de usuario 206. Sus secuencias se pueden cruzar para que se afecten entre sí, ya sea de forma idéntica o dispar. En el ejemplo ilustrado, los dos resonadores 100, 206 se pueden comunicar entre sí para comenzar el enmarañamiento. Las secuencias 102, 204 se cruzan y se combinan a través de una o más fórmulas de combinación, véanse los ejemplos anteriores, para proporcionar una o más secuencias secundarias 208.

Otro ejemplo de CE, como se ilustra en la figura 6, es considerar múltiples secuencias 102A-1, 102A-2, 102A-3 de múltiples resonadores de baliza 100A-1, 100A-2, 100A-3, todos los cuales desean acoplarse. La primera baliza 100A-1 transmite "aaaaaaaaaaa...", la segunda baliza 100A-2 transmite "22222222222222..." y la tercera baliza 100A-3 transmite "??????????????????..." La nueva secuencia secundaria combinada 208 de únicamente los resonadores de baliza n.º 1 y n.º 2, 100A-1, 100A-2, puede ser una secuencia alterna "a2a2a2a2a2" o una secuencia de Fibonacci "aa2aa2aaa2aaaa2aaaaaaaa2..." o cualquier otro operador. La secuencia secundaria 208 puede ser modificada adicionalmente entonces por la tercera secuencia de baliza 102A-3. En la secuencia simple, la derivada puede ser "a2?a2?a2?a2?..." o incluso desplazar en el tiempo la tercera secuencia 102A-3 "aa2aa2aaa2aaaa2?aaaaaaaa2?..."

Antes de pasar a un ejemplo de uso de CE para encriptar un mensaje entre Alice y Bob, en la figura 7 se ilustra otro ejemplo de una característica, conocida como "llamada". Las llamadas permiten la inserción de la secuencia única 205 del usuario en la secuencia de RC 102 normal. Aunque la secuencia de usuario 205 puede ser única y no aleatoria, debería tener todas las características de una secuencia aleatoria para evitar disminuir la entropía de la secuencia de RC pura. Un ejemplo es el hash único de un usuario, que es en gran medida indistinguible de cualquier secuencia aleatoria de números junto con una firma de tiempo, se inserta en una secuencia de radiodifusión de RC en vivo 102 y es detectable para los destinatarios potenciales con conocimiento del hash. La secuencia de usuario 205 puede ser detectable por cualquier otro usuario que conozca su existencia y que esté supervisando la secuencia de RC.

La secuencia de usuario 205 se puede usar como una señal que inicia las comunicaciones con otros participantes para comenzar una sesión o intercambio seguro. Múltiples usuarios pueden generar señales similares de forma simultánea para crear un identificador multiparte, iniciando también un comunicado o sesión segura.

Volviendo a la figura 7, Alice 202A y Bob 202B han establecido un protocolo en el que Bob 202B puede supervisar la secuencia 102 del resonador 100 para esperar la secuencia de usuario 205A de Alice para saber que Alice está enviando un mensaje y comenzar la generación de claves. En el presente caso, Alice 202A inserta su secuencia de usuario 205a "x37Q" en la secuencia 102. Bob, que normalmente no interacciona con el resonador, sino que solo supervisa la secuencia 102 percibe la secuencia de usuario 205A y comienza un algoritmo de generación de claves predeterminado.

Se pueden usar hashes simples, y combinarlos con firmas dependientes del tiempo para que la misma secuencia de números de identificador nunca se vuelva a ver en la secuencia de RC, pero los usuarios autorizados siempre pueden ser capaces de detectar su valor único. Esto puede señalizar a un individuo o grupo que un usuario está intentando llamar o establecer contacto o entregar un mensaje. Las combinaciones de hashes también se pueden usar de la misma manera en múltiples secuencias en combinaciones complejas para lograr el mismo efecto mientras se ofuscan adicionalmente los comunicadores y se perturba el funcionamiento normal del resonador 100.

La señalización criptográfica puede ser la base para usar el resonador 100 como una señal portadora para que una red de comunicaciones llame o haga ping a los usuarios. La combinación de los pings de múltiples resonadores 100 puede ser, por ejemplo, el mensaje de alerta para usar un conjunto específico de los resonadores 100 para comunicarse. La secuencia de usuario 205 y sus comunicaciones subsiguientes se pueden solapar u operar de manera independiente - un conjunto de resonadores 100 solo se puede usar para "llamar" al contacto previsto, mientras que un sistema diferente puede transportar la transferencia de datos o las comunicaciones reales.

Esta construcción no se limita a su uso para la identificación y llamada. También se puede usar para difundir un mensaje de alerta a un individuo o grupo de usuarios autorizados. Esto es equivalente a usar la secuencia de RC 102 para insertar esteganografía en lugar de establecer contacto, pero usa un mecanismo casi idéntico.

Volviendo a un ejemplo de CE para encriptar un mensaje entre Alice y Bob, para comenzar, ambos tienen su propia secuencia de usuario 205. Los ejemplos de sus secuencias de usuario 205 pueden ser un número grande, un número grande relacionado con un hash de su dirección de correo electrónico o cualquier otra secuencia de dígitos. La secuencia de usuario 205, en algunos ejemplos, es lo suficientemente larga y / o aleatoria como para que no se pueda distinguir de ninguna otra secuencia de números aleatorios. Nuevamente quieren intercambiar mensajes encriptados 106 a las 01:00 UTC. Alice se comunica con el resonador 100 y tiene su secuencia de usuario 205A insertada en la secuencia 102. Bob conoce la secuencia de usuario de Alice 205A y tiene su aparición en la secuencia secundaria 208 como una señal procedente de Alice para comenzar a grabar la secuencia 102. Bob vuelve así, al insertar su secuencia de usuario 205B en la secuencia 102 para que Alice la identifique y comience el esquema de encriptación que idearon.

En este ejemplo, la secuencia 102 es "1111111111111111", la secuencia de usuario de Alice es "3333" y la secuencia de usuario de Bob es "7777". Además, su secuencia acordada para comenzar a usar la secuencia es "956888". Para cualquiera que esté supervisando las comunicaciones, todo lo que ven es "11111111133339568881111111111117777956888111111111111..." Obsérvese que, en realidad, estos son números aleatorios largos que no se repiten, pero simplemente se simplifican para este ejemplo. Nadie debería ser

capaz de adivinar que "3333" es la secuencia de usuario de Alice, y Bob solo lo sabe ya que la conoce, siendo lo opuesto cierto para la secuencia de usuario de Bob. Para cualquier observador externo, estos son solo más números aleatorios en la secuencia. "956888" puede ser una instrucción acordada, desde una tan fácil como "comenzar a grabar" a "usar cada 7-ésimo dígito para crear el esquema de encriptación e insertar el mensaje encriptado de vuelta a la secuencia".

En otros ejemplos, Alice y / o Bob también pueden hacer que su resonador de usuario 206 inserte más dígitos aleatorios en la secuencia principal 102 para confundir y enmarañar adicionalmente sus comunicaciones. Esto permite a Alice y a Bob comunicarse indirectamente a través de la perturbación del resonador 100. Todo lo anterior parece una secuencia de números aleatorios a un observador externo, todo ello mientras se proporciona a Alice y a Bob la capacidad de encriptar y desencriptar fácilmente la información con muy poca potencia de cómputo.

Dado lo anterior, a continuación se muestra un ejemplo de encriptación práctica de un mensaje usando la CE. Alice y Bob acuerdan usar solo un resonador 100 independiente y cada uno se enmaraña con él al insertar su propia secuencia de usuario 204, y la secuencia secundaria 208 resultante se usa para encriptar mensajes. Alice y Bob comienzan al identificarse con el resonador y entre sí. La secuencia de usuario 205 de Alice es "6325" y la secuencia de usuario 202 de Bob es "7458". El resonador de usuario 206 de Alice genera una secuencia de usuario 204 de repetición de "1234", mientras que Bob genera una secuencia repetitiva de "5678". El resonador 100, a la hora acordada 01:00 UTC, transmite 4 dígitos aleatorios de "8542". El mensaje de Alice a Bob es "9999", pero dado que Alice y Bob han afectado a la secuencia 104 para crear una secuencia secundaria 208, ambas se usan para encriptar la secuencia.

Así, a las 01:00 + 1 UTC, las dos secuencias de usuario y la secuencia se acoplan para identificar en primer lugar las partes y comenzar la creación de la clave. En este ejemplo, por adición falsa:

6325 (secuencia de usuario de Alice)
7458 (secuencia de usuario de Bob)
8542+ (números aleatorios del resonador)
1215

Y así, "1215" se transmite a las 01:00 + 1 UTC. Nuevamente, esto parece simplemente otra sección aleatoria de la secuencia, pero dado que tanto Alice como Bob conocen sus propias secuencias de usuario y las del otro, y leen los dígitos de la secuencia, saben que es hora de comenzar a crear la clave para encriptar el mensaje.

A la hora 01:00 + 2 UTC, la secuencia a partir del resonador es entonces una secuencia secundaria 208 para Alice y Bob (para el resto del mundo, estos solo lo ven como la secuencia). El resonador 100 genera los siguientes 4 números aleatorios "1182" y eso se enmaraña con las dos secuencias de usuario, como a continuación:

1234 (secuencia de usuario de Alice)
5678 (secuencia de usuario de Bob)
1182+ (números aleatorios del resonador)
7084

La secuencia "7084" es entonces la clave 104 usada para encriptar y desencriptar el mensaje de Alice de "9999":

9999
7048+
6937

El mensaje encriptado 106 de "6937" se puede transmitir sin problemas a Bob sin preocuparse de que este sea puesto en peligro. Sin embargo, Bob puede desencriptarlo con exactamente la misma facilidad, ya que él generó de forma simultánea su clave simétrica al mismo tiempo que Alice generó la suya.

Alice y Bob saben que han acoplado sus resonadores de usuario 206 al resonador 100 disponible debido a la primera señal de secuencia de usuario que cambió la secuencia para identificar que se debería generar una clave nueva y que está por llegar un mensaje. Una vez que se ha intercambiado la información inicial entre Alice y Bob, y obsérvese que la clave no se ha intercambiado, todo lo que ambas partes han de hacer es supervisar las secuencias acordadas para saber cuándo generar una clave nueva y que se esté comunicando un mensaje. Obsérvese también que entonces, cada ida y vuelta entre Alice y Bob se puede encriptar usando una clave diferente, generada sobre la marcha. Incluso si un atacante pudiera obtener una cualquiera de las claves, esto solo es bueno para el mensaje en cuestión.

En otros ejemplos, Alice y Bob pueden verificar en la práctica la independencia del resonador 100, y que están verdaderamente acoplados al mismo, al enviar una señal de validación 210, que puede ser, en un ejemplo, la suma falsa de sus secuencias de usuario 204, y comparar esta con la secuencia 102. Cualquiera de ellos puede enviar la señal de validación 210 de forma independiente y por separado entre sí. Si el resonador 100 se ve puesto en peligro,

uno o ambos verán una señal no aleatoria cuando reconstruyan la secuencia real 102. Alice y / o Bob también pueden ofuscar adicionalmente sus comunicaciones al enviar una serie de únicamente señales de validación 210 (dígitos aleatorios) antes de enviar su secuencia de usuario 205. Esto puede confundir a un pirata informático que solo está buscando una conexión con el resonador como desencadenante para la generación de claves.

Sobre la base de los ejemplos previos, la figura 8 ilustra otro ejemplo de RC más. Esta característica, conocida como Cascada de Conexiones de Criptografía, es una propiedad criptográfica grupal en la que se establecen conexiones mutuas entre usuarios fiables que desean comunicarse. Se puede crear una secuencia única de etapas entre los usuarios 200 para intercambiar fragmentos pequeños de datos de baja encriptación para generar un efecto de bola de nieve a un estado resonante de encriptación fuerte.

En un ejemplo simple, se puede usar un modelo circular en donde el primer miembro de un grupo, Alice 202A, anuncia que se pueden usar dos resonadores de baliza 100A-1, 100A-2 para encriptar las comunicaciones para el grupo. Alice 202A entra en contacto con Bob 202B al combinar su propia secuencia de usuario 204A con los das secuencias públicas 102A-1, 102A-2. Bob 202B responde a Alice 202A añadiendo su propia secuencia de usuario 204B para validar este nuevo canal, pero también transmite instrucciones nuevas a Charlie 202C acerca de cómo combinar las secuencias públicas 102A-1, 102A-2 para el grupo. Este proceso se itera entre todos los usuarios del grupo (ilustrados hasta Zoe 202Z) hasta que la secuencia de usuario 204 de todos, generada por cada uno de sus generadores personales 206, se incorpore a las secuencias públicas 102A-1, 102A-2 y a todos los usuarios (de Alice a Zoe).

Las cascadas de resonadores 100 también se pueden establecer independientemente de los usuarios 200 para crear perturbaciones dentro de la red 300. Esto se puede usar para inicializar nuevas secuencias de resonador 100 o alterar el estado de cualquier grupo conectado en red de resonadores 100. Esto se puede usar como una medida de seguridad adicional para reducir el impacto de cualquier número de elementos puestos en peligro dentro del grupo en red.

Los problemas con cualquiera de los resonadores criptográficos 100A, 100B, 100C, etc., pueden ser que uno o más de los resonadores 100 no sean lo suficientemente "aleatorios", de forma deliberada o por carencia de diseño. La figura 9 ilustra un ejemplo de criptografía recursiva. La recursión combina unas secuencias actuales / futuras 102 con unas secuencias previas 108 al insertar las secuencias previas 108 de forma aleatorizada en la secuencia en vivo 102. Los ejemplos se pueden lograr de cualquier número de formas con el tiempo y la distancia desde la secuencia en vivo actual 102 de vuelta a la secuencia histórica 108. La inserción de esta secuencia histórica 108 en la secuencia en vivo 102 se puede realizar en tiempo real o lograrse mediante la intercalación aleatoria de la secuencia histórica 108 en la secuencia en vivo 102. Esto complica y aleatoriza la secuencia recursiva 112 desde el generador recursivo 110 cuando, por ejemplo, el generador de pseudo-números es débil y posiblemente defectuoso. Se ha observado que algunos conjuntos de chips y algoritmos adolecen de este defecto, que se puede mitigar hasta cierto punto mediante el uso de la recursión, idealmente a partir de múltiples resonadores 100 dentro de una red 300. La recursión criptográfica también se puede usar para retransmitir la misma señal una y otra vez mientras parece diferente para el usuario no autorizado. Esto puede ser útil en las situaciones en las que una señal criptográfica no hace "ping" al usuario objetivo, como en el ejemplo de llamada anterior, ya que su dispositivo está apagado o es temporalmente disfuncional. La señal recurrente sigue estando presente hasta que es detectada por el usuario objetivo, pero por lo demás está ofuscada y es, aparentemente, una secuencia de números aleatorios de evolución normal a partir del resonador recursivo 111.

Otro ejemplo de una técnica para mitigar los resonadores 100 defectuosos o posiblemente puestos en peligro puede ser la Criptografía Recombinante. Los ejemplos combinan múltiples secuencias 102 a partir de múltiples resonadores 100 en una secuencia recombinante de secuencia 114 nueva y única. Esto puede difundir cualquier elemento no aleatorio anterior con el tiempo. La figura 10 ilustra un ejemplo de formación de una secuencia recombinante 114. Las secuencias públicas 102A-1, 102A-2... 102A-n a partir de los resonadores de baliza 100A-1, 100A-2... 100A-n son recopiladas, por ejemplo por un servidor y realiza una función o funciones únicas f(n)A-1, f(n)A-2... f(n)An que, en el ejemplo ilustrado, son multiplicar la primera secuencia 102A-1 por 32,75, multiplicar la segunda secuencia 102A-2 por 1,223 y multiplicar la n-ésima secuencia 102A-n por 11.972. Esto forma unas secuencias modificadas 102A-1', 102A-2'... 102A-n' que se combinan entonces usando una función recombinante $F_{rc}(n)$ para difundir entonces una secuencia recombinante 114, por ejemplo a través de un resonador de radio 100B. En este ejemplo, la función recombinante $F_{rc}(n)$ es una suma de cada una de las secuencias modificadas, con cada secuencia siendo nuevamente multiplicada por una función. Cualquiera de las funciones f(n)A-1, f(n)A-2... f(n)An, $F_{rc}(n)$ puede ser tan simple como una constante entera aplicada usando funciones matemáticas básicas (suma, resta, multiplicación, división, exponente, factorial, etc.) o cálculos algebraicos complejos con números complejos o irracionales.

En una comparación del mundo real, la Criptografía Recombinante es análoga a combinar múltiples gases similares en una gran cámara de gas, mezclando así el gas del producto y dificultando la identificación de los componentes individuales. Otros ejemplos pueden combinar la Criptografía Recombinante con la Criptografía Recursiva, y esto puede eliminar en la práctica cualquier secuencia no aleatoria. Esto es análogo a la combinación de dos gases de volúmenes variables y a la creación de un tipo completamente nuevo de gas molecular, dejando algunos de los

gases originales sin mezclar para complicar adicionalmente la mezcla. Esto crea un tipo de problema informático que no es diferente de hacer una espectroscopía de masas generalizada sobre un gas idealizado - sin grandes recursos informáticos ni esfuerzo, es difícil identificar y deconstruir los componentes de este tipo de gas, que no está en equilibrio, ni es homogéneo, ni está en homeostasis en relación con la materia prima de secuencias criptográficas nuevas. También es, en esencia, más complejo que la espectroscopía básica ya que este sistema es como tener un número inagotable de moléculas y elementos nuevos, muchos de los cuales solo se verán una vez y nunca más. Por lo tanto, es resistente a la caracterización y al análisis de patrones / frecuencias ya que es dinámico y evoluciona con el tiempo.

Otra variante ilustrativa para combinar o modificar las secuencias 102 del resonador 100 es la Criptografía de Viaje en el Tiempo. Este ejemplo, ilustrado en la figura 11, puede ser un esquema de reencriptación continua en donde cualquier conjunto de datos en vivo se recicla constantemente a través de cualquier combinación de resonadores criptográficos 100. Por ejemplo, una hoja de cálculo de datos privados 302 se puede poner en línea y facilitarse a través de un sitio web de cara al público y, por lo tanto, la hoja de cálculo de datos públicos 304. Una o más de las entradas de datos V_{xy} (en donde x e y son la fila y la columna del valor, respectivamente) se pueden encriptar usando la criptografía de viaje en el tiempo y las entradas de datos encriptados V_{xy}' cambian continuamente en un ciclo o programación - de forma individual o agregada. Como se ilustra, la función $F_{tt}(n)$ dicta el valor encriptado V_{xy}' de cada entrada de datos. El valor encriptado V_{xy}' puede cambiar con cada dígito que pasa en las secuencias 102 o volver a cifrarse en alguna tabla de tiempo estática o continua (de ahí el "viaje en el tiempo"). Además, cada entrada de datos V_{xy} se puede encriptar usando una función simple o compleja diferente.

Por lo tanto, las entradas de datos V_{xy} fluyen a través del tiempo como entradas de datos encriptados V_{xy}' siempre cambiantes a medida que los datos evolucionan con cualquier secuencia criptográfica. Esta también aísla los datos públicos en vivo frente a cualquier puesta en peligro pasada de una secuencia criptográfica controlada o descifrada por un actor mal intencionado. Este modelo obligaría a cualquiera que intente descodificar una secuencia en vivo a registrar todos los datos cambiantes durante un periodo de tiempo prolongado, al mismo tiempo que hace esto mismo para todas las secuencias criptográficas resonantes en vivo sospechosas que soporten la encriptación de estos datos. Esta agota los recursos enemigos al tiempo que hace que a los usuarios autorizados les resulte sencillo el acceso a los mismos datos en público. También se puede modificar rápidamente sobre la marcha.

Otro ejemplo adicional de la invención implica la introducción de una cadena no aleatoria de dígitos, una secuencia "fantasma" 212, generada por un resonador fantasma 114, en una secuencia de resonador 102 para formar una secuencia o secuencias integradas fantasma 116. El usuario 200 no necesita manipular matemáticamente la secuencia o secuencias integradas fantasma 116, la propia secuencia fantasma 212 es la comunicación. Para leer la secuencia fantasma 212, un usuario puede tener un filtro "fantasma" 214 para extraer la secuencia fantasma 112 de la secuencia o secuencias integradas fantasma 116 y leer el mensaje.

La secuencia fantasma 112 se puede introducir en cualquier secuencia de resonador 102 al incorporar información aparentemente aleatoria en la secuencia o secuencias 102 desde un resonador fantasma 114. La secuencia fantasma 212 puede ser reconocida y usada por usuarios autorizados 200 que usan el filtro fantasma 214 para verla o capturarla. La secuencia fantasma 212 usa la secuencia de resonador 102 para formar la secuencia integrada fantasma 116 para actuar como una señal portadora para una secuencia paralela de información que, a nivel superficial, parece idéntica a una secuencia de resonador ordinaria 102.

La figura 12A ilustra lo anterior y un ejemplo de una comunicación entre Alice y Bob 202A, 202B. Alice 202A quiere enviar un mensaje a Bob 202B, e introduce ese mensaje en su resonador fantasma 114. El resonador fantasma 114 inserta entonces partes del mensaje en un mensaje de texto sin formato. Este puede ser un mensaje estático (que actúa entonces como un mensaje codificado 106) o, por ejemplo, insertarse en una o más secuencias de resonador 102 para formar una o más secuencias integradas fantasma 116. Bob 202B descarga el mensaje 106 o graba las secuencias 116, aplica el filtro 214 y lee el texto.

La figura 12B ilustra otro ejemplo. Volviendo a lo anterior, Alice 202A quiere enviarle a Bob 202B el mensaje "hola", el cual, cuando se convierte en números por posición en el alfabeto, es 8-4-12-12-15. El resonador fantasma 114 de Alice comienza la tarea de comunicarse con tres resonadores de baliza 100A-1, 100A-2, 100A-3 e insertar la secuencia fantasma 212 (que es, en este ejemplo, 8412125) en sus múltiples secuencias 102A-1, 102A-2, 102A-3 para formar múltiples secuencias integradas fantasma 116A-1, 116A-2, 116A-3. Bob 202B aplica el filtro fantasma 214, extrae la secuencia fantasma 212 de las secuencias integradas fantasma 116A-1, 116A-2, 116A-3 y recibe el "hola" de Alice.

La criptografía fantasma se distingue de la criptografía enmarañada anterior, ya que, en un ejemplo, el mensaje se envía en claro, solo que dividido en fragmentos muy pequeños y enviado poco a poco a través de una o más secuencias y oculto en ellas. En un ejemplo de papel y lápiz, usando "hola", las formas previas de la criptografía intercambian una letra por otra y se ha de conocer la clave para desencriptar el mensaje. Como de lo anterior, Alice puede escribir en un trozo de papel "imsmu" (que, convertido de nuevo en texto, es 9-13-19-13-21) y entregarlo a Bob. Solo Bob conoce el mensaje, ya que él es el único que tiene la clave. Cualquiera que intercepte el mensaje lo conoce encriptado. La criptografía fantasma actúa de manera diferente, Alice, en lugar de enviar "imsmu" a Bob, le

escribe a Bob una nota:
"Altura correcta, todo según la programación, el pozo está seco y se nos acabó la tinta".
Para todos los observadores, esta es una comunicación de texto sin formato, sin embargo, Bob aplica un filtro, que en papel y lápiz puede ser tan simple como una superposición con la posición de letra indicada, y puede obtener por filtrado "Altura correcta, todo según la programación, el pozo está seco y se nos acabó la tinta".

Aunque se destaca la diferencia en papel y tinta, el uso de las secuencias de resonancia 102 es mucho más potente. En el ejemplo de secuencia, Alice envió a Bob tres "notas" simultáneas (una a partir de cada baliza 102) y Bob extrajo el mensaje de todas esas tres. Obsérvese que se podría elegir cualquier número de balizas.

Para aumentar la fuerza criptográfica de cualquiera de los ejemplos previos, múltiples ejemplos se pueden disponer en capas uno encima de otro. Por ejemplo, una vez que se encripta un mensaje, este también se puede convertir entonces en fantasma. Se puede desarrollar un protocolo en el que informar a una parte homóloga acerca de un mensaje entrante ocurre usando secuencias a partir de un conjunto de resonadores, la clave de encriptación se crea sobre la marcha usando un segundo conjunto independiente o parcialmente independiente de secuencias de resonador, y el mensaje encriptado se convierte en fantasma a través de un tercer conjunto de resonadores. El uso de la computación moderna para desarrollar ese protocolo es relativamente sencillo, sin embargo, muy pocos o ningún actor mal intencionado tiene los recursos para vulnerar un protocolo de codificación de este tipo.

Otra característica de la presente invención es la Criptografía de Punto de Control. Una red de valla geográfica local 302 de los resonadores 100 se puede disponer para aislarse de otros resonadores públicos o privados 100A, 100B, 100C o sus redes, para usarse como un perímetro criptográfico para los usuarios en un espacio vallado geográficamente. Una valla geográfica, en términos generales en el presente documento, puede ser una demarcación física o lógica en torno a un grupo de usuarios. Una definición menos general es una barrera virtual en torno a un área geográfica física usada para fines administrativos. En el presente documento, la definición se amplía para incluir barreras sobre un dominio virtual, tales como un grupo lógico de usuarios conectados que pueden estar dispersos geográficamente a nivel global, pero que tienen acceso a la misma red de valla geográfica 302.

En un ejemplo, una serie de resonadores criptográficos locales 100D está idealmente desconectada de cualquier red de comunicaciones 300, de forma equivalente a una LAN. Estos resonadores criptográficos locales 100D pueden formar un área de valla geográfica 304 usada para vallar geográficamente un grupo de usuarios 200 y asegurar sus comunicaciones de red localizadas. Si la proximidad física o lógica de un usuario a los resonadores criptográficos locales 100D se extiende más allá de los límites del área de valla geográfica 304, en un ejemplo, ir más allá del alcance de señal de los resonadores criptográficos locales 100D, los usuarios 200 pierden en la práctica el acceso a las comunicaciones encriptadas del grupo. Los ejemplos permiten que las áreas de valla geográfica 304 se superpongan para crear espacios de trabajo complejos de acceso para usuarios autorizados.

La figura 13 ilustra algunos ejemplos de criptografía de punto de control. En este ejemplo, hay dos áreas de valla geográfica 304, el área de valla geográfica alfa 304A y el área de valla geográfica beta 304B. Los usuarios 200-1, 200-2, 200-3 y 200-4 están dentro del área de valla geográfica alfa 304A basándose en su proximidad al resonador criptográfico local alfa 100D-1. Los usuarios 200 dentro del área de valla geográfica alfa 304A solo tienen permitido acceder al servidor alfa 10A. En este ejemplo, el servidor alfa 10A no está conectado a red externa 300 alguna, es decir, Internet (lo que también se conoce como "con separación de aire"), sino solo a la red de valla geográfica 302.

En otros lugares, los usuarios 200-11, 200-12, 200-13 y 200-14 están dentro del área de valla geográfica beta 304B en función de su proximidad al resonador criptográfico local alfa 100D-1 y al resonador criptográfico local beta 100D-2. Los usuarios 200-11, 200-12, 200-13, 200-14 solo tienen permitido acceder al servidor beta 10B. Obsérvese que los usuarios no pueden recibir la señal del resonador criptográfico alfa local 100D-1, lo que los excluye del área de valla geográfica alfa 304A. Ambos conjuntos de usuarios 200-1, 200-2, 200-3, 200-4, 200-11, 200-12, 200-13, 200-14 tienen permitido acceder al centro de datos 12.

Obsérvese que los usuarios 200-3, 200-4, 200-12 y 200-14, mientras están dentro de sus respectivas áreas de valla geográfica 304A, 304B, no tienen conexiones a Internet. En este ejemplo, las conexiones de la red externa 300 no afectan a si un usuario 200 está "dentro", o no, de las áreas de valla geográfica 304A, 304B. Otros ejemplos pueden tener en cuenta las conexiones de red externas de un usuario como parte de los requisitos para estar en un área vallada geográficamente 304. Por ejemplo, en el área de valla geográfica alfa 304A, dado que el servidor alfa 10A tiene separación de aire, el hecho de que los usuarios 200-1 y 200-2 estén conectados a Internet (o cualquier otra red no segura 300) puede descalificarlos de acceder al servidor alfa 10A, cortándolos así del área de valla geográfica alfa 304A, a pesar de que pueden recibir la secuencia 102 del resonador criptográfico local alfa 100D-1.

Obsérvese que solo el acto físico de "recibir" la secuencia 102 del resonador criptográfico local 100D no es la condición indispensable de estar en el área de valla geográfica 304. Las secuencias de resonador 102 todavía se siguen usando para crear texto de cifrado y claves criptográficas 104. Sin acceso a la secuencia particular del resonador criptográfico local 100D (y la información acerca de cómo usarlo), un usuario "externo" no tiene acceso, en esencia, a la OTP que se usa para asegurar los datos en el área vallada geográficamente 304. Por lo tanto, cualquier usuario 200 cercano al resonador criptográfico local 100D puede enviar y recibir texto de cifrado que este

puede desencriptar dentro de esta valla geográfica / valla criptográfica. La frontera de la valla criptográfica actúa como un punto de control (de ahí el nombre) en donde la pérdida de señal para el resonador criptográfico local 100D equivale a perder la capacidad de desencriptar el texto de cifrado, incluso si el texto de cifrado está disponible de alguna manera.

Los ejemplos que requieren proximidad física pueden ser triviales de implementar en redes WiFi, ya que el tiempo de desplazamiento no nulo de la señal se puede usar para establecer coherencia. Los usuarios distantes 200 pueden experimentar latencia incluso en una red no repetidora. La adición coherente de múltiples señales dentro del área de valla geográfica 304 se logra fácilmente ya que la temporización de la señal es idéntica para alguna distancia física definida a partir de la constelación de resonadores criptográficos locales 100D. Puntos adicionales, o aquellos que capturan la señal a partir de un repetidor, no pueden recrear la correlación de la combinación de señales dentro de la valla geográfica.

Se pueden lograr geometrías adicionales para vallas geográficas lógicas, en donde las firmas de tiempo se incluyen en la señal de los resonadores criptográficos locales 100D dentro de este marco. En este ejemplo, la proximidad física no es un problema ya que el tiempo se puede sincronizar electrónicamente después de que se establezca una señal almacenada en memoria intermedia y capturada dentro del grupo de usuarios vallados geográficamente.

Dados los diversos ejemplos de esquemas criptográficos bosquejados anteriormente, estos conducen a toda una serie de otras soluciones y configuraciones criptográficas, y una de tales soluciones es la Criptografía de Ámbar. Esta solución permite que cualquier dato encriptado estático en reposo y la clave de desencriptación adjunta se almacenen por separado y se faciliten a usuarios fiables en el futuro. La solución puede ser en la práctica una instantánea en el tiempo de una cantidad fija de datos encriptados que no evoluciona ni cambia con el tiempo. Los datos se pueden almacenar en el dominio público ya que la secuencia criptográfica resonante 102 exacta usada para crearlos se destruyó en el pasado y solo fue conservada por los usuarios de confianza 200. Solo estos usuarios pueden leer los datos almacenados en este estado de tipo ámbar.

La figura 14 ilustra que el almacenamiento de ámbar 216 puede registrar en un momento particular una o más secuencias 102A, 102B, 102C de uno o más resonadores criptográficos 100A, 100B, 100C. En un ejemplo, el tiempo se puede elegir como el tiempo en el que se encriptaron los datos. Estos segmentos de secuencia pueden almacenarse como el segmento sin procesar, un segmento de secuencia secundaria 208 o la clave misma. Cuando se almacena como secuencia sin procesar o secuencia secundaria, se pueden aplicar diferentes algoritmos criptográficos a las secuencias almacenadas, lo que permite que un almacenamiento de ámbar 216 sirva a múltiples conjuntos de datos encriptados sin que cada conjunto comparta la misma clave. El almacenamiento de ámbar puede ser cualquier memoria no transitoria, incluyendo cualquier forma o memoria magnética o de estado sólido, cinta magnética, almacenamiento óptico, etc. El almacenamiento de ámbar 216 pueden ser uno o más dispositivos de almacenamiento, propiedad de uno o más usuarios. En la situación de "clave" múltiple, puede ser que no se requiera la clave, sino las secuencias archivadas en ámbar. En la figura 14, un ejemplo puede ser que un usuario separado almacene cada una de las secuencias separadas, pero que el algoritmo de encriptación usara todas las tres secuencias para encriptar los datos. Ningún usuario tiene entonces suficientes de las secuencias para desencriptar por sí solo los datos. El usuario no tiene de por sí la clave, sino una porción de los datos necesarios para generar la clave. Esto es importante, ya que incluso si un actor mal intencionado pudiera recopilar todas las secuencias necesarias, este sigue sin tener la clave, se sigue necesitando que el algoritmo de encriptación sea conocido. Por lo tanto, para una seguridad adicional, solo un 4º usuario puede tener el algoritmo.

La solución criptográfica de ámbar no es diferente a publicar un archivo encriptado grande en el dominio público, en donde cualquiera puede descargarlo, pero solo aquellos con la clave pueden abrirlo. En un ejemplo, la "clave" es la combinación de secuencia de resonador única que no se repite, pero que puede ser distribuida en cualquier momento por quienes la capturaron. La clave 104 también puede ser una combinación de múltiples claves mantenidas por diferentes usuarios para crear una única clave maestra - esto es análogo a crear una caja fuerte que requiere varias llaves que funcionan al unísono para abrirla. Estas claves 104 pueden ser mantenidas por numerosos usuarios de confianza, todos los cuales han de acordar descifrar los datos al mismo tiempo.

Ampliando el ejemplo anterior, la combinación de redes de RC y resonadores individuales 100 puede formar una Variedad Criptográfica. A nivel global, las estructuras más grandes son las variedades criptográficas (CM), que se pueden conectar para formar un superespacio criptográfico. Cada variedad criptográfica se define localmente como una colección de resonadores 100 y redes conectadas que pueden estar enlazadas a otros resonadores o redes para formar una superficie virtual discreta. La superficie puede tener un número arbitrario de dimensiones efectivas n, de forma análoga a la dimensión de cualquier variedad. Cada conexión es un punto de acceso potencial para transmitir las OTP. Los puntos en la variedad criptográfica no están limitados por la proximidad física. Por ejemplo, una única variedad criptográfica puede ser la colección enlazada de resonadores en órbita basados en satélites 100 conectados a resonadores terrestres y submarinos 100, que transmiten por secuencias desde plataformas de hardware y software. Una segunda variedad similar con estructuras paralelas puede estar adyacente a la primera, pero solo tiene puntos de intersección o superposición a través de conexiones y comunicaciones por satélite directas. Aunque ningún usuario puede alcanzar puntos internos entre las dos variedades criptográficas, puede seguir intercambiando información y resonar por los puntos de intersección.

Las CM pueden asumir el marco matemático de cualquier variedad, solo limitado por los requisitos topológicos de la red que crean estos - virtual o física. La colección de CM que crean una red criptográfica puede ser fractal, jerárquica o caótica con el tiempo. Las CM pueden surgir naturalmente o por diseño para satisfacer las necesidades criptográficas de la comunidad de dispositivos a los que dan servicio. Por lo tanto, las CM iniciales más grandes pueden quedar subsumidas por variedades derivadas y, con el tiempo, ser reemplazadas por las mismas para volverse, ellas mismas, unas CM nuevas. Una jerarquía de las CM se puede volver fractal o generar una red caótica nueva, posiblemente independiente del punto de origen. El punto importante es que las CM son capaces de soportar gráficos conectados de forma múltiple de cualquier número de dimensiones. En este sentido, en las escalas de las más grandes a las más pequeñas, las CM cubren todas las manifestaciones posibles de un sistema de RC. Nuevamente, estas son comunicaciones por cualquier medio, no simplemente redes basadas en IP o sus variantes digitales. Por ejemplo, las señales generadas por RC se pueden crear usando modulación en fase o en cuadratura, codificación diferencial y otros esquemas para transmitir datos de cualquier tipo.

También se encuentra disponible, usando ejemplos de la presente invención, la Rotura de Simetría Criptográfica. Esto permite a los usuarios 200 comunicarse entre sí de manera segura y cualquier intruso que quiera "escuchar" en la conversación. En este contexto, el estado criptográfico simétrico de un sistema dinámico de resonadores 100 y usuarios 200 es uno en el que no hay dispositivos que estén inicialmente enlazados o "acoplados" entre sí. En el presente caso, dinámico significa que los resonadores 100 y los usuarios 200 tienen la capacidad de interaccionar entre sí. Es decir, los usuarios 200 no están simplemente escuchando de forma pasiva las secuencias de resonador 102 y usándolas. Estos usan sus propias secuencias personales 204 para alterar el estado de las secuencias públicas 102 y las que pertenecen a otros usuarios 200, como se indica en los ejemplos anteriores.

En este sistema, y por simplicidad, todos los dispositivos tienen acceso a todas las secuencias 102 y otros dispositivos y pueden elegir conectarse o no (por supuesto, este no tiene que ser el caso, y es igualmente aceptable cualquier combinación más general). El estado de simetría rota se produce cuando cualquier grupo de usuarios decide conectarse entre sí y acoplarse a cualquier número de resonadores 100 para comenzar a comunicarse de forma segura. La red criptográfica de todas las mezclas posibles de este sistema se ha concretado en una configuración específica para esta sesión segura. Esto incluye el algoritmo dinámico a usar para la sesión. Con cada usuario adicional que desee unirse, la red segura ha de interrumpirla para hacerse visible y comenzar a comunicarse. Esta interrupción cambia la configuración de las comunicaciones a un nuevo estado de simetría rota, alertando en esencia a todos los miembros de la presencia y disponibilidad del usuario nuevo para participar en un intercambio seguro. También evita la escucha clandestina ya que nadie puede recopilar las comunicaciones en texto claro sin participar en la encriptación usada para asegurarlas.

Esta propiedad es importante por dos razones, una de las cuales son los cimientos para las comunicaciones cuánticas. Los comunicadores seguros sabrían de forma instantánea cuándo cualquier parte de la señal descifrada queda disponible para un usuario nuevo - de lo contrario, no hay forma alguna de capturar de forma pasiva la señal no encriptada. Ver / escuchar / leer cualquier cosa requiere un acoplamiento al sistema de una manera detectable, perturbándolo así a un estado nuevo de "simetría rota". En segundo lugar, los estados tanto simétrico como roto se pueden usar para la autenticación y validación de cualquier red segura, antes de transmitir cualquier información. Si el grupo de usuarios no se pueden, todos ellos, acoplar entre sí y con los resonadores 100 seleccionados, estos no son usuarios autorizados o de confianza mutua. Si, de alguna manera, un actor malo intentara entrar a la fuerza en el grupo en cualquier momento, esto desestabilizaría la simetría rota y nadie sería capaz de ver cosa alguna. Las comunicaciones mueren y el grupo inicializa una nueva sesión segura, excluyendo el punto de entrada que se intentó, tal como un dispositivo de usuario 103 o un resonador 100 pirateado.

Obsérvese que los ejemplos anteriores se pueden concretar en uno o más conceptos criptográficos como la Convergencia Criptográfica. Esto es como muestran los ejemplos anteriores en una red de resonadores muy pública (por ejemplo, unas balizas 100A y / o unos resonadores de radio 100B) sin acceso alguno a un resonador privado (por ejemplo, unos resonadores de radio 100B y / o seguros 100C), un grupo de usuarios puede compartir el acceso a múltiples secuencias públicas 102A y las secuencias 204 generadas por sus propios dispositivos para crear una secuencia privada temporal única construida sobre la confianza de sus propios dispositivos - estos pueden incluso querer publicar sus propias identidades o avalar de otro modo su fiabilidad. Esto se puede hacer en software en un dispositivo cualquiera dentro del grupo o en un entorno de nube en espacio aislado. Esta secuencia que se ha hecho converger tiene múltiples usos más allá de asegurar todo el grupo y superar cualquier desconfianza de los resonadores públicos 100A, 100B (por ejemplo, si estos fueron pirateados y puestos en peligro con dígitos no aleatorios). Los subgrupos de usuarios 200 se pueden establecer restando la secuencia de cualquier usuario de la secuencia que se ha hecho converger, usando asimismo, posiblemente, un algoritmo diferente. Esto es como tener un nuevo recurso comunitario al crear un espacio de reunión virtual para acceder a la criptografía. Esta es la base para crear una estructura o red más grande de puntos de convergencia similares que pueden formar una retícula o un espacio de fase - esto se puede hacer incluso si cada resonador primario 100 es malo. Este entorno virtual es una forma de capturar todos los estados posibles de los puntos de convergencia y usarlos como un sistema de encriptación distribuido dinámico.

Cualquier trayectoria a través de los puntos de esta retícula es como elegir una clave de encriptación de transmisión

por secuencias para conectar a los usuarios o abrir un canal de comunicaciones seguro. Este evita el fallo de cualquier parte del sistema o, por ejemplo, que caiga todo un país o región geográfica de resonadores 100. Los esquemas criptográficos de confianza se pueden crear más allá de la RC mediante el uso de una red distribuida de dispositivos virtuales secundarios, algunos de los cuales, o todos ellos, pueden ser certificados en la práctica por grupos de usuarios. Por ejemplo, se puede crear una autoridad de certificación para SSL para la seguridad de IP normal, sin tener un servicio centralizado para hacerlo. A diferencia de las cadenas de bloques en uso para bitcoin, no existe registro permanente alguno de las transacciones y firmas usadas por nadie ni es necesario que los mismos puntos de convergencia existan a lo largo del tiempo. Se pueden rotar arriba y abajo según sea necesario a petición. Los usuarios no están bloqueados en el uso de uno cualquiera o una combinación de puntos y pueden perder la confianza en algunos. La cuestión es que no son elementos fijos permanentes y no hay un único punto de confianza, incluso dentro del modelo de RC.

Los ejemplos de la presente invención también pueden dar como resultado una Jerarquía criptográfica. Esta propiedad de la RC permite a muchos usuarios 200 del mismo conjunto de datos tener grados variables de privilegios. Aunque puede darse acceso a todo al director general (o al cuerpo directivo) de una empresa, bajo este sistema criptográfico, pueden permitirse accesos menores a los empleados de nivel inferior dentro del mismo marco criptográfico. Esto es importante ya que no cambia la fuerza criptográfica del sistema ni requiere, de hecho, la implementación de recursos informáticos adicionales. Todos o algunos de los elementos de RC del mismo sistema se pueden usar para crear un nivel de acceso escalonado o cualquier modelo complejo que emita derechos a los datos. Al cambiar el acceso a los resonadores 100 (por ejemplo, vallado geográfico) y / o alterar el algoritmo usado para encriptar datos con ellos, se puede establecer cualquier sistema personalizado de privilegios sobre el mismo conjunto de datos sin crear múltiples conjuntos de datos encriptados. Cada usuario tiene un filtro criptográfico efectivo por el cual puede ver el conjunto de datos global, restringiendo su visibilidad según sea necesario su conocimiento.

Una vez que se adopta un sistema de RC, un problema es su uso por actores mal intencionados. El cifrado perfecto permite a estos actores enviar asimismo comunicaciones seguras. La misma seguridad que protege la información "buena" también evita que las fuerzas del orden vulneren las comunicaciones en busca de información "mala". Sin embargo, esto no es necesariamente cierto, existen varias técnicas ampliamente usadas para que las fuerzas del orden público aprovechen el sistema del actor mal intencionado. Si una agencia autorizada tiene acceso físico al dispositivo del actor mal intencionado, se pueden descubrir los protocolos anteriores y la policía puede tener acceso completo a las comunicaciones. Si la misma agencia puede acceder de forma simultánea a todas las mismas secuencias, incluyendo las secuencias privadas, y obtienen acceso al algoritmo usado para combinarlas, pueden ver todas las comunicaciones en claro. Esto sucede en la actualidad cuando se usan algoritmos simples y / o deficientes - una agencia puede examinar rápidamente el espacio de claves pequeño generado para desencriptar las comunicaciones - sin saber cosa alguna de antemano acerca del algoritmo. Este es un ataque por fuerza bruta poco sofisticado contra un mal sistema de seguridad diseñado para mantener alejados a los piratas informáticos ordinarios, y a los buenos.

Sobre los pilares de la RC, la información se puede transmitir como metadatos ligeramente encriptados con una única cadena que define cada parámetro - un hash SHA-2 simple puede lograr esto. Una cadena ilustrativa se puede parecer a:
[firma de hora / fecha en GMT] [identificador personal] [lista de resonadores a usar] [combinación de sesión de resonadores a usar] [conjunto de instrucciones de seguridad adicionales} [etc.]

Cada parte en las comunicaciones puede intercambiar y comparar las instrucciones, o una parte puede hacer esto, pero cada intercambio debería usar la misma función de hash para verificar la autenticidad. Estas son inherentemente muy fuertemente resistentes a la colisión, ya que el primer bloque nunca se repetirá y la combinación de sesión puede ser una función muy compleja. Estas son variables dependientes del tiempo y el espacio, a diferencia de las claves estáticas en la práctica usadas en la actualidad en la PKI.

Al abordar otros defectos potenciales de la RC, un actor malo puede crear y desplegar sus propios resonadores, pero no hay garantía alguna de que los usuarios usen sus resonadores, o únicamente sus resonadores, cuando se encripta un mensaje. Además, al revisar el uso de la creación de secuencias derivadas y la combinación de secuencias con secuencias de resonador, un defecto potencial puede ser que un actor malo desborde uno o más resonadores con una gran porción de π (o e, etc.). El número es no repetitivo, pseudoaleatorio e infinito, pero sus valores están documentados a un billón de dígitos. Esto no es verdaderamente una opción, ya que un actor malo no puede "desbordar" un resonador existente. El resonador sigue generando su propia secuencia.

Un pirata informático puede poner en peligro el hardware / software del resonador, pero no puede crear una secuencia falsa y engañar a las personas para que lo usen - a menos que haya pirateado los dispositivos de confianza. La "suplantación" de un resonador es análoga a la suplantación de un encaminador, y esta es una puesta en peligro diferente de la red, no la fortaleza del sistema de RC. Como ejemplo, los resonadores pueden usar una convención de nomenclatura de IP similar como encaminadores. Los delincuentes pueden desplegar y nombrar sus resonadores malos para que se parezcan a un resonador válido, pero para fines bancarios y similares, habría una lista blanca de resonadores. Obsérvese que el poder de la RC es que cualquiera que use cualquier número de

resonadores malos aún puede vencer el pirateo informático de los delincuentes simplemente al usar un único resonador válido en su algoritmo. Es decir, si un usuario encripta usando un resonador malo unas secuencias 1 - 9 pero usara un algoritmo seguro para generar una secuencia válida 10, las comunicaciones siguen siendo seguras. Además, incluso si todas las secuencias 1 - 10 fueran malas y no verdaderamente aleatorias, un algoritmo bien diseñado sigue produciendo una encriptación fuerte.

Por lo tanto, las comunicaciones seguras siguen siendo posibles en un entorno completamente puesto en peligro usando esta técnica. Más allá de tener una clave de identificación segura, cada usuario también puede tener un algoritmo único - estas son funciones complejas triviales que generar y hay una diversidad infinita de las mismas. Esto es análogo a que cada usuario obtenga su propia clave única y su propio juego de cerraduras único - su tipo de clave solo encaja en su tipo de cerradura y no hay dos usuarios que tengan la misma combinación.

El cálculo retroactivo tampoco es factible. El análisis criptográfico funciona mejor con grandes conjuntos de datos estructurados, usando repetidamente la misma clave en cifrados de bloques, por ejemplo. Esto funciona ya que las letras "s" y "a" son más comunes en texto sin formato que "q" y "z" - las tablas de probabilidad están bien estudiadas para todos los idiomas. Ni siquiera esta información es útil en el presente caso, ya que un usuario nunca reutiliza la misma clave. Un problema de cálculo mucho más difícil es tomar entonces todas las secuencias de resonador que producen claves de longitud variable, comparar estas con todo el texto de cifrado de longitud variable y confiar en hacer el mismo análisis criptográfico. La dificultad crece de forma exponencial cuando se usan números (por ejemplo, para transacciones bancarias) en donde la distribución de los números está, en gran medida, diseminada por igual en 0 - 9. El problema es el mismo que en lo anterior, se requiere una información casi perfecta acerca de todo el sistema desde el resonador al algoritmo de usuario final. Absolutamente todo conduce a cualquier texto sin formato.

Pasando a las transacciones bancarias y de punto de venta, aunque muchos pueden usar secuencias de resonador públicamente disponibles al 100 %, algunos de estos pueden ser dispositivos de proximidad - por ejemplo, estos solo transmiten a no más de 20 pies (6,01 m) de una caja registradora, y no están conectados a Internet. Otros sistemas basados en abono para aplicaciones son muy fáciles de implementar y validar a través de las tecnologías existentes - la RC puede ser simplemente una capa adicional de cifrado muy fuerte por un coste muy bajo en energía y recursos informáticos. De cualquier manera, la mecánica de las aplicaciones individuales es bastante sencilla.

Las opciones más avanzadas, como el enmarañamiento, responden dinámicamente a cada dispositivo de una manera única - un actor malo tendría que obtener un control total sobre ambos extremos para ver algo, pero en ese momento, ya posee todo aquello a lo que tienes acceso. Si ya ha puesto en peligro por completo tu dispositivo, la criptografía no puede ayudar a asegurar las comunicaciones. Recuérdese que incluso un resonador suplantado o puesto en peligro es insuficiente para descifrar la RC. Sin embargo, como toda seguridad, esto puede abrir ligeramente los algoritmos más débiles al análisis criptográfico, pero eso también requiere que el texto de cifrado se capture en grandes cantidades. Los algoritmos fuertes pueden tener variables dinámicas dependientes del tiempo, coordenadas de GPS, dirección de IP, etc., que amplían enormemente los recursos necesarios para aplicar ingeniería inversa al algoritmo (suponiendo que el actor malo tenga acceso completo a todas las secuencias de resonador usadas y al texto de cifrado).

La figura 15 ilustra un ejemplo de la configuración básica de hardware para un resonador 400. El resonador 400 puede incluir un generador de números aleatorios 402. El RNG 402 puede incluir al menos uno de un generador de números aleatorios verdaderos, un generador de números pseudoaleatorios o cualquier secuencia no repetitiva de números que tenga una característica de una secuencia de números aleatorios. Como anteriormente, el generador de números aleatorios 402 puede generar una primera secuencia de números aleatorios 404. El resonador 400 puede incluir un transmisor 406 que se puede acoplar eléctricamente al generador de números aleatorios 402. El transmisor 406 transmite la primera secuencia 404 de números aleatorios al menos por radiofrecuencia o a través de una red. El resonador 400 también puede incluir un receptor 408 para recibir secuencias de números 410 a partir de otros dispositivos analizados a continuación. Un experto en la materia entiende fácilmente que el transmisor 406 y el receptor 408 pueden ser, en algunos ejemplos, uno en el mismo elemento, un transceptor. Este incluye cualquier procesamiento requerido para o bien enviar o bien recibir las secuencias 404, 410.

También se puede incluir un procesador 412 que integra una segunda secuencia 410 de números en la primera secuencia 404 de números aleatorios para formar una secuencia combinada y una memoria de resonador no transitoria 414 para almacenar datos. La segunda secuencia de números 410 se puede recibir desde un segundo resonador u otro dispositivo de usuario analizado a continuación.

La figura 16 ilustra un comunicador 500 que se puede usar para comunicarse con el resonador 400 y otros dispositivos de usuario. Las comunicaciones en el contexto de la presente invención incluyen recibir secuencias de números aleatorios a partir de uno o más resonadores 400, transmitir números de comunicador al resonador 400 y comunicarse con otros comunicadores para intercambiar texto sin formato y comunicaciones encriptadas y el algoritmo para generar una clave de encriptación.

Para facilitar estas capacidades, el comunicador tiene un receptor de comunicador 502 que puede recibir la primera

secuencia 404, así como un motor criptográfico de comunicador 504 que se puede enlazar electrónicamente al receptor de comunicación 502. El motor criptográfico 504 también puede incluir una memoria no transitoria 506 y un procesador 508 enlazado electrónicamente a la memoria. Un ejemplo de las tareas 504 del motor criptográfico de comunicador puede ser leer al menos una porción de la primera secuencia 404 y convertir la porción de la primera secuencia 404 en una clave criptográfica 104.

En ejemplos adicionales, puede haber un segundo o más comunicadores como parte del sistema, estos comunicadores adicionales pueden tener más o menos capacidades que el comunicador 500 descrito anteriormente. Cuando el primer comunicador se comunica con el segundo, por ejemplo, cuando Alice se comunica con Bob, como se describe en los muchos ejemplos anteriores, el primer y el segundo procesadores de comunicador 508 tienen un algoritmo común para convertir independientemente la porción de la primera secuencia 404 en la clave criptográfica 104. Esta es una de las ventajas de la invención, ni Alice ni Bob tienen que compartir una clave, cada uno genera la suya de forma independiente. Esta clave también se genera solo en el momento en el que se necesita, por lo que no está almacenada, esperando para desbloquear datos en el futuro. Esto aumenta la seguridad ya que, al no ser necesario transmitir la clave, esta no puede ser interceptada. Asimismo, dado que se genera sobre la marcha para cada conjunto de datos, la posesión de una clave antigua no permite la desencriptación de ningún dato futuro o dato pasado distinto de los datos para los que se generó la clave.

Para incluir algo de hardware en los ejemplos anteriores, como ya se ha indicado, el receptor de comunicador 502 puede recibir una segunda secuencia de números 416 desde un segundo resonador. La memoria no transitoria 506 puede almacenar al menos una porción de la segunda secuencia 416. El procesador de comunicador 508 puede leer entonces la porción de la segunda secuencia 416 y usa ambas porciones 404, 416 para crear la clave criptográfica 104.

Otros ejemplos hacen que el comunicador 500 también incluya un generador de números de comunicador 509 que pueda generar un número de comunicador 510. El generador de números de comunicador 509 puede ser un RNG como se ha descrito anteriormente, para generar secuencias aleatorias o pseudoaleatorias 410 a insertar en la secuencia de un resonador 400. El generador de números de comunicador 509 también puede generar secuencias no aleatorias que se pueden usar para identificar el comunicador 500 o, en coordinación con el motor criptográfico 504, para insertar mensajes, como se describe a continuación.

El comunicador 500 también puede incluir un transmisor de comunicador 512 que transmite el número de comunicador 410, 510 al resonador 400. El receptor de resonador 408 recibe el número de comunicador 410, 510; y el procesador de resonador 412 puede integrar el número de comunicador 410, 510 en la secuencia de números aleatorios 404 para formar una secuencia combinada 416 que puede ser transmitida por el transmisor 402.

En otros ejemplos indicados anteriormente, una vez que el número de comunicador 510 se inserta en una secuencia de resonador combinada 416, un segundo comunicador 500 puede recibir la secuencia combinada 416 y detectar el número de comunicador 510. Una vez así informado, el segundo comunicador puede generar su propio (un segundo) número de comunicador. El primer 510 y el segundo números de comunicador se pueden enviar entonces al resonador 400 para combinarse con la secuencia de resonador 404 para hacer una segunda secuencia combinada que puede ser transmitida por el transmisor 402.

Aún otros ejemplos de RC involucraron la temporización de las secuencias. Así, el transmisor de resonador 402 puede transmitir una porción de la primera secuencia en un instante T0. Esta primera secuencia de T0 puede ser grabada, ya sea por un segundo dispositivo (como un comunicador 500) o por el propio resonador 400. Independientemente de qué dispositivo la grabe, la primera secuencia de T0 se puede almacenar en la memoria del resonador 414 (es decir, ya estaba allí si el resonador la grabó, o puede recibirla nuevamente a través del receptor 408 cuando se grabara en otro lugar). El procesador 412 puede combinar entonces la primera secuencia de T0 con una porción de la primera secuencia en un instante T1 para formar una secuencia recursiva 112 que se transmite entonces.

Otros ejemplos que usan la temporización de las secuencias incluyen un conjunto de datos 302 que tiene al menos un valor VI. En el presente caso, el resonador 400 transmite una porción de la primera secuencia en un instante T0 y el motor criptográfico de comunicador 504 puede encriptar el valor VI usando la primera secuencia de T0. El resonador 400 también puede transmitir una porción de la primera secuencia en un instante T1. Esto puede permitir que el motor criptográfico de comunicador 504 descifre el valor V1 usando la primera secuencia de T0 y vuelva a cifrar el valor VI usando la primera secuencia de T1. La criptografía de ámbar, como se ha indicado anteriormente, es otro ejemplo de uso de un segmento de tiempo de una secuencia. Una memoria no transitoria de ámbar puede almacenar la primera secuencia de T0 y un conjunto de datos se puede encriptar usando la primera secuencia de T0.

Más ejemplos del uso de múltiples resonadores 400 y / o múltiples comunicadores 500 pueden dar como resultado la secuencia recombinante 114 descrita anteriormente. En el presente caso, el segundo resonador transmite una segunda secuencia de números 416 y el comunicador 500 puede recibir la primera y la segunda secuencias 404, 416. El motor criptográfico de comunicador 504 puede combinar la primera y la segunda secuencias 404, 416 para

formar la secuencia recombinante 114 que puede ser transmitida por el primer transmisor de comunicador 512. La secuencia recombinante 114 se puede formar habitualmente cuando el primer motor criptográfico de comunicador 504 aplica un algoritmo, en un ejemplo Frc(n), a la primera y la segunda secuencias 404, 416, para formar la secuencia recombinante 114.

Otros ejemplos pueden dar como resultado comunicaciones "fantasma". En el presente caso, el primer número de comunicador 510 puede ser un mensaje en texto claro transmitido al resonador 400 usando una primera secuencia para formar la "secuencia fantasma" combinada 212 de la primera secuencia 404 y la primera secuencia del primer número de comunicador 510. Entonces, un segundo comunicador puede recibir la secuencia fantasma 212 y su motor criptográfico 504 aplica el filtro 214 que filtra el primer número de comunicador 510 de la secuencia fantasma 212. Obsérvese que se puede usar cualquier número de resonadores 400 y sus secuencias para dividir entre ellos el mensaje.

También se pueden analizar los ejemplos de vallas geográficas. En el presente caso, el transmisor de resonador 402 es un transmisor de corto alcance y un alcance de señal de transmisor define un área de valla geográfica 304. Cuando el receptor de comunicador 502 recibe la primera secuencia de números 404 dentro del área de valla geográfica, el motor criptográfico de comunicador 504 puede crear la clave criptográfica 104 necesaria para acceder a cualesquiera conjuntos de datos o hardware que sean parte del área de valla geográfica 304. A la inversa, cuando el comunicador 500 está fuera del área de valla geográfica 304, por ejemplo, ya no puede recibir la señal de transmisor, el motor criptográfico de comunicador 504 no puede crear la clave criptográfica 104. Esto se puede observar fácilmente, ya que si un usuario no puede acceder al resonador adecuado, nunca tendrá toda la información necesaria para leer la información encriptada.

Los siguientes ejemplos describen los métodos de uso de RC en etapas. Obsérvese que estas etapas pueden ser realizadas por el hardware analizado en el presente documento y se pueden materializar en hardware especialmente diseñado o en software que se ejecuta en hardware habitual o patentado.

La figura 17 ilustra un ejemplo de un método para encriptar y desencriptar datos usando criptografía resonante, estas son las etapas básicas del resonador 100, que incluyen generar una primera secuencia de números aleatorios usando el resonador 400 (la etapa 1000) y, entonces, transmitir la primera secuencia de números usando un transmisor 402 (la etapa 1002). La figura incluye adicionalmente el método de enmarañamiento básico, que puede incluir las etapas de recibir, en el resonador 400, la segunda secuencia de números 410 (la etapa 1004). La primera secuencia y la segunda secuencia 404, 410 se pueden combinar, usando un procesador 412 en el resonador 400, para formar una secuencia combinada 208 (la etapa 1006) y, entonces, transmitir la secuencia combinada 208 con el transmisor 402 (la etapa 1008).

La figura 18 ilustra algunos de los ejemplos que involucran al comunicador 500. En el presente caso, el método incluye recibir la primera secuencia 402 en un comunicador 500 (la etapa 1010) y, entonces, almacenar al menos una porción de la primera secuencia 402 en la memoria 506 del comunicador (la etapa 1012). El procesador 508 del comunicador puede convertir la porción de la primera secuencia 402 en una clave criptográfica 104 (la etapa 1014). Esto se puede hacer usando un algoritmo.

Añadir al menos un comunicador 500 más permite que dos partes se comuniquen de manera segura. Este método hace que el segundo comunicador reciba la primera secuencia 402 (la etapa 1016) y almacene una porción de la misma (la etapa 1018). El segundo comunicador 500 puede convertir la porción de la primera secuencia en la misma clave criptográfica 104 usando el mismo algoritmo (la etapa 1020). Como anteriormente, esto permite que Alice y Bob se comuniquen usando la misma clave, pero generada de forma independiente y, en algunos ejemplos, sobre la marcha.

Un ejemplo del uso de múltiples resonadores se ilustra en la figura 19. El comunicador 500 puede recibir la segunda secuencia de números 416 generada por un segundo resonador 400 (la etapa 1022) y almacenar al menos una porción de la misma (la etapa 1024). Las porciones de la primera y la segunda secuencias 402, 416 se pueden convertir en una clave criptográfica usando un algoritmo (la etapa 1026).

La combinación de las secuencias del resonador 400 y el comunicador 500 es un ejemplo de un método de convergencia, como se ilustra en la figura 20. Este ejemplo hace que el resonador 400 reciba el número de comunicador 410, 510 generado por el primer comunicador (la etapa 1028). Esta etapa se toma desde el punto de vista del resonador, pero en otros ejemplos puede ser fácilmente el caso que el comunicador 500 generara el número de comunicador 410, 510 y lo transmitiera al resonador 400. Sin embargo, puede ser que el resonador 400 combine el número de comunicador 410, 510 con la primera secuencia 402 en una secuencia combinada 416 (la etapa 1030) y, entonces, la transmita (la etapa 1032).

Continuando con el ejemplo anterior, esta secuencia combinada permite a Alice señalizar (o más) a Bob en secreto. Este método incluye recibir, en un segundo comunicador, la secuencia combinada 416 (la etapa 1034) y, entonces, almacenar al menos una porción de la misma (la etapa 1036). El procesador del segundo comunicador 508 puede detectar la porción del número de comunicador 410, 510 a partir de la secuencia combinada 416 (la etapa 1038).

La figura 21 ilustra un ejemplo de un método de conexión en cascada. En este método, el resonador 400 recibe (o recibe de vuelta) un segundo número de comunicador generado por el segundo comunicador y el primer número de comunicador, ambos transmitidos por el segundo comunicador (la etapa 1040). El resonador 400 combina el primer y el segundo números de comunicador con la primera secuencia en una segunda secuencia combinada (la etapa 1042) y, entonces, la transmite (la etapa 1044).

Además, la figura 22 ilustra un método para formar la secuencia recombinante 114. El primer comunicador 500 recibe entonces la primera secuencia 402 (la etapa 1046) y la segunda secuencia 410 de números (habitualmente generada por un segundo resonador) (la etapa 1048). Las dos secuencias se alteran y / o se combinan usando alguna forma de algoritmo para convertir así una porción de la primera y la segunda secuencias en la secuencia recombinante 114 (la etapa 1050). La secuencia recombinante 114 se transmite con un primer transmisor de comunicador 512 (la etapa 1052).

Las figuras 23 - 25 ilustran ejemplos en los que se toman segmentos de la secuencia en momentos diferentes para obtener resultados criptográficos más avanzados. Para una secuencia recursiva 112, un ejemplo de un método incluye generar una primera secuencia de números aleatorios en un instante T0 usando el resonador (la etapa 1054). Una porción de la primera secuencia de T0 se almacena en una memoria no transitoria (la etapa 1056). Este almacenamiento puede ser en el mismo resonador 400 que generó la primera secuencia de T0, un resonador diferente o un comunicador 500. Independientemente de dónde se almacene, la primera secuencia de T0 se envía de vuelta al resonador para combinarse con una porción de la primera secuencia en un instante T1 para formar una secuencia recursiva (la etapa 1058) que se transmite entonces (la etapa 1060). Véase la figura 23.

Otro método de segmentos de tiempo, ilustrado en la figura 24, permite que valores separados disponibles públicamente se encripten con el tiempo. En este método, el comunicador 500 recibe la primera secuencia de T0 (la etapa 1062) y encripta un primer valor de datos VI usando la primera secuencia de T0 (la etapa 1064).
Separada en el tiempo, entonces el comunicador 500 recibe del resonador una primera secuencia de T1 (la etapa 1066). El valor de datos VI se puede desencriptar entonces usando la primera secuencia de T0 (la etapa 1068) y encriptarse entonces usando la primera secuencia de T1 (la etapa 1070).

Un ejemplo de tiempo más es la criptografía de ámbar. En el presente caso, un ejemplo de un método incluye generar una primera secuencia de números aleatorios en un instante T0 usando el resonador (la etapa 1054) (como anteriormente). La primera secuencia de T0 se almacena en una memoria de ámbar (la etapa 1072) y se usa para encriptar un conjunto de datos (la etapa 1074). Sin embargo, una vez encriptado de esta manera, no hay forma de que un actor malo escuche en busca de la secuencia de T0, se pierde en el tiempo.

La RC fantasma puede ser otra herramienta potente. Esta se puede usar para enviar texto claro en secuencias públicas, Bob solo necesita saber qué secuencias y qué segmentos son segmentos fantasma a partir del segmento público de las secuencias. Esta también puede enviar un mensaje encriptado para acrecentar su enturbiamiento. La figura 26 ilustra un ejemplo de este método al generar, en el primer comunicador, un primer número de comunicador 510 que es un mensaje en texto claro (la etapa 1076). El primer número de comunicador se puede transmitir al resonador 400 usando una primera secuencia (la etapa 1078). El primer número de comunicador se combina con la primera secuencia para dar una secuencia fantasma en el resonador 400 (la etapa 1080). El segundo comunicador recibe la secuencia fantasma 116 (la etapa 1082) y la filtra para extraer el primer número de comunicador de la secuencia fantasma 116 (la etapa 1084).

Otro ejemplo puede conducir a un método de vallado geográfico de un área para restringir el acceso a datos. Un ejemplo, ilustrado en la figura 27, define el área vallada geográficamente 304 basándose en el alcance de señal del transmisor que transmite la primera secuencia (la etapa 1086). Una vez definida, se puede permitir (la etapa 1088) o denegar (la etapa 1090) el acceso a los datos de vallador geográfico basándose en la recepción de la primera secuencia en el primer comunicador. Si se recibe la primera secuencia, se puede crear la clave criptográfica usada para desencriptar los datos en el área vallada geográficamente (la etapa 1092).

También se ha de entender que la mención de una o más etapas de método no excluye la presencia de etapas de método adicionales o etapas de método intermedias entre las etapas expresamente identificadas. De manera similar, también se ha de entender que la mención de uno o más componentes en un dispositivo o sistema no excluye la presencia de componentes adicionales o componentes intermedios entre los componentes expresamente identificados.

Cualquiera o todos los transmisores o receptores anteriores pueden actuar en concierto como un transceptor y pueden ser compatibles con uno o más de identificación por radiofrecuencia (RFID), comunicación de campo cercano (NFC), Bluetooth®, Bluetooth® de baja energía (BLE), LiFi, WiFi™, ZigBee®, protocolos de comunicaciones de retrodispersión ambiental (ABC) o tecnologías similares. Los resonadores y / o comunicadores pueden incluir hardware, firmware y / o software que permita que sus procesadores se comuniquen con otros dispositivos a través de redes cableadas o inalámbricas, ya sean de área local o extensa, privadas o públicas, según sea entendido por los expertos en la materia. La información recibida (secuencias, algoritmos, etc.) puede ser procesada por uno o más

procesadores informáticos según se desee en diversas implementaciones de la tecnología divulgada, y / o almacenada en uno o más dispositivos de memoria.

Un procesador puede incluir uno o más de un microprocesador, microcontrolador, procesador de señales digitales, coprocesador o similares, o combinaciones de los mismos, capaces de ejecutar instrucciones almacenadas y operar sobre datos almacenados. Las memorias pueden incluir, en algunas implementaciones, uno o más tipos de memoria adecuados (por ejemplo, tales como memoria volátil o no volátil, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de solo lectura programable (PROM), memoria de solo lectura programable y borrable (EPROM), memoria de solo lectura programable y borrable eléctricamente (EEPROM), discos magnéticos, discos ópticos, disquetes flexibles, discos duros, cartuchos extraíbles, memoria flash, una serie redundante de discos independientes (RAID), y similares). La memoria puede almacenar archivos que incluyen un sistema operativo, programas de aplicación (incluyendo, por ejemplo, una aplicación de navegador web, un motor de miniaplicaciones o accesorios, y /u otras aplicaciones, según sea necesario), instrucciones ejecutables y datos.

Dados los conceptos anteriores, el hardware y el software que ejecutan la RC se pueden variar en todo el espectro de los dispositivos de IoT. Estos incluyen servidores que son autónomos (por ejemplo, con una separación de aire) o que están conectados en red a uno o más comunicadores. La red 300 puede incluir una o más redes conmutadas por paquetes, tal como una red basada en protocolo de Internet (IP), una red de área local (LAN), una red de área extensa (WAN), una red de área personal (PAN), una intranet, Internet, una red celular (por ejemplo, GSM (Sistema Global para Comunicaciones Móviles), CDMA (Acceso Múltiple por División de Código), WCDMA (CDMA de Banda Ancha), LTE (Evolución a Largo Plazo), IEEE 802.11x, etc.), una red de fibra óptica, u otro tipo de red que sea capaz de transmitir datos. La red 300 puede incluir una red conmutada por circuitos, tal como una red telefónica pública conmutada (PSTN) para proporcionar servicios telefónicos para teléfonos tradicionales.

El resonador y / o el comunicador pueden incluir uno o más dispositivos que se comunican con la red 300 o entre sí. Por ejemplo, el resonador y / o el comunicador pueden incluir un televisor que incluya aplicaciones (por ejemplo, Internet Explorer®, Chrome®, etc.) y una interfaz de comunicación (por ejemplo, una interfaz de comunicación por cable o inalámbrica) para conectarse a la red. El resonador y / o el comunicador también pueden incluir uno o más dispositivos que se comunican con la red para proporcionar un servicio de Internet. Por ejemplo, estos pueden incluir un ordenador de escritorio, un ordenador portátil, un ordenador de mano, un ultraportátil, tableta, teléfono inteligente, etc., u otros tipos de dispositivos de comunicación. Los servidores pueden alojar una página web a la que puede acceder un usuario usando los comunicadores.

Dado que muchos dispositivos descritos anteriormente ya tienen incorporado un generador de números pseudoaleatorios, un chip o software que integra la RC, para formar un resonador 100, puede tener una nueva propiedad: la capacidad de recibir múltiples secuencias de resonador externas diferentes y combinarlas usando un conjunto programable de fórmulas. También ha de tener la capacidad de combinar esta salida con el equivalente a texto sin formato (datos no encriptados) como una secuencia de datos encriptados, usando también cualquier cosa desde la adición modular hasta esquemas más complejos, e invertir el proceso para la desencriptación. Este puede ser un chip autónomo o parte de un SOC. El chip tendría todas o un cierto subconjunto de las propiedades criptográficas de RC anteriores y, posiblemente, integraría un conjunto de instrucciones reducido de funciones matemáticas, usando idealmente baja energía.

Una característica más avanzada permitiría que las secuencias de entrada / salida del resonador fueran tanto analógicas como digitales. Cualquier hardware puede armonizar las diferentes formas de secuencias de resonador y las funciones requeridas para su uso. Por ejemplo, un dispositivo que acepte secuencias de resonador a partir de un esquema de encriptación de RC de desplazamiento de fase se podría combinar con una secuencia basada en IP para crear una nueva transmisión analógica de radiodifusión. El hardware se puede diseñar para dar servicio a una cámara de entrada / salida de mezclado para todas las formas de resonadores y sus tecnologías concomitantes para crear nuevas secuencias de resonador por sí mismos.

Las configuraciones de red híbrida que usan la RC pueden usar circuitos de RC programables tanto en transmisores como en receptores como un canal criptográfico efectivo para asegurar las comunicaciones. El ejemplo más simple sería una red de radio digital encriptada en donde una malla segura privada se podría crear dinámicamente para establecer un centro de comunicaciones cerrado y encriptado. La complejidad de la construcción de dispositivos de usuario final seguros y de la conmutación de infraestructura se reduce en gran medida junto con los requisitos de energía del dispositivo móvil para participar en este tipo de red híbrida. Por analogía, se puede crear cualquier solución híbrida para aprovechar la eficiencia de RC, en especial cuando la plataforma RC está integrada como una solución de hardware programable en transición sin problemas entre entornos operativos.

Las descripciones contenidas en el presente documento son ejemplos de realizaciones de la invención y no pretenden limitar en modo alguno el alcance de la invención. Como se describe en el presente documento, la invención contempla muchas variaciones y modificaciones de un sistema de criptografía resonante. Asimismo, hay muchas variaciones posibles en el diseño y las configuraciones de los resonadores. Estas modificaciones serían evidentes para los expertos en la materia a la que se refiere la presente invención y se pretende que estén dentro del alcance de las reivindicaciones que siguen. Por ejemplo, un experto en la materia reconocerá que las

instrucciones ejecutables se pueden almacenar en un medio de almacenamiento no transitorio y legible por ordenador, de manera que, cuando son ejecutadas por uno o más procesadores, hace que uno o más procesadores implementen los métodos descritos anteriormente.

En esta descripción se han expuesto numerosos detalles específicos. Se entiende, no obstante, que las implementaciones de la tecnología divulgada se pueden poner en práctica sin estos detalles específicos. En otros casos, no se han mostrado en detalle técnicas, estructuras y métodos bien conocidos para no enturbiar la comprensión de esta descripción. Las referencias a "un ejemplo", "ejemplo adicional", "diversos ejemplos", "algunos ejemplos", etc., indican que el ejemplo o ejemplos de la tecnología divulgada así descrita pueden incluir un rasgo distintivo, estructura o característica particular, pero que no todos los ejemplos incluyen necesariamente el rasgo distintivo, estructura o característica particular. Además, el uso repetido de la expresión "en un ejemplo" no se refiere necesariamente al mismo ejemplo, aunque puede ser el caso.

De principio a fin de la memoria descriptiva y de las reivindicaciones, los siguientes términos adoptan al menos los significados explícitamente asociados en el presente documento, a menos que el contexto indique claramente lo contrario. El término "o" pretende significar un "o" inclusivo. Además, los términos "un", "una" y "el / la" pretenden significar uno o más, a menos que se especifique lo contrario o quede claro por el contexto que se dirige a una forma singular. Por "comprender" o "contener" o "incluir" se pretende indicar que al menos el elemento o etapa de método que se nombra está presente en el artículo o método, pero no excluye la presencia de otros elementos o etapas de método, incluso si los otros elementos o etapas de método tienen la misma función que lo que se nombra.

Como se usa en el presente documento, a menos que se especifique lo contrario, el uso de los adjetivos ordinales "primero", "segundo", "tercero", etc., para describir un objeto común, indica simplemente que se está haciendo referencia a diferentes casos de objetos similares, y no se pretende implicar que los objetos así descritos deban estar en una secuencia dada, ya sea de forma temporal, espacial, en una clasificación o de cualquier otra manera.

Además, las secuencias se indican de principio a fin como números aleatorios o generadas a partir de RNG. Sin embargo, en este contexto, y como se ilustra, la secuencia puede no ser simplemente secuencias de números, esta puede ser cualquier carácter, letra o dígito, en cualquier idioma o alfabeto apropiado, de árabe, a binario, cirílico o griego.

Ciertas implementaciones de la tecnología divulgada se describen anteriormente con referencia a diagramas de bloques y de flujo de sistemas y métodos y / o productos de programas informáticos de acuerdo con implementaciones ilustrativas de la tecnología divulgada. Se entenderá que uno o más bloques de los diagramas de bloques y/o diagramas de flujo, y las combinaciones de los bloques en los diagramas de bloques y/o diagramas de flujo, se pueden implementar, respectivamente, mediante instrucciones de programa ejecutables por ordenador. De forma similar, algunos bloques de los diagramas de bloques y diagramas de flujo pueden no requerir necesariamente realizarse en el orden presentado, se pueden repetir o pueden no requerir necesariamente realizarse en absoluto, de acuerdo con algunas implementaciones de la tecnología divulgada.

Aunque ciertas implementaciones de esta divulgación se han descrito en relación con lo que actualmente se consideran las implementaciones más prácticas y diversas, se ha de entender que esta divulgación no se limita a las implementaciones divulgadas, sino que, por el contrario, pretende cubrir diversas modificaciones y disposiciones equivalentes incluidas dentro del alcance de las reivindicaciones adjuntas. Aunque se emplean términos específicos en el presente documento, estos se usan únicamente en un sentido genérico y descriptivo y no para fines de limitación.

Esta descripción escrita usa ejemplos para divulgar ciertas implementaciones de la tecnología y también para permitir que cualquier experto en la materia ponga en práctica ciertas implementaciones de esta tecnología, incluyendo la fabricación y uso de cualquier aparato o sistema y la realización de cualquier método incorporado. El alcance patentable de determinadas implementaciones de la tecnología se define en las reivindicaciones, y puede incluir otros ejemplos que se les ocurran a los expertos en la materia. Se pretende que tales otros ejemplos estén dentro del alcance de las reivindicaciones si estos tienen elementos estructurales que no difieran del lenguaje literal de las reivindicaciones, o si incluyen elementos estructurales equivalentes con diferencias insustanciales con respecto al lenguaje literal de las reivindicaciones.

REIVINDICACIONES

1. Un sistema para comunicaciones seguras usando encriptación de datos, comprendiendo el sistema:

una colección de dispositivos (100A, 100B, 100C) para generar una pluralidad de secuencias continuas de datos (102A, 102B, 102C), comprendiendo cada dispositivo:

un generador de números aleatorios que comprende al menos uno de un generador de números aleatorios verdaderos, un generador de números pseudoaleatorios y cualquier secuencia no repetitiva de números que tenga una característica de una secuencia de números aleatorios, en donde cada generador de números aleatorios está configurado para generar una secuencia de números aleatorios; y
un transmisor, acoplado eléctricamente a uno de los generadores de números aleatorios, configurado para transmitir una primera secuencia generada de números aleatorios dentro de un área vallada geográficamente;
un primer comunicador (103) que comprende:

un primer receptor de comunicador configurado para recibir la primera secuencia;
un primer motor criptográfico de comunicador, enlazado electrónicamente al primer receptor de comunicación, y que comprende:

una memoria no transitoria que almacena al menos una porción de la primera secuencia; y
un primer procesador de comunicador enlazado electrónicamente a la memoria para leer al menos una porción de la primera secuencia y para convertir la porción de la primera secuencia en una clave criptográfica,

en donde el transmisor es un transmisor de corto alcance y un alcance de señal de transmisor del transmisor de corto alcance define el área vallada geográficamente;
en donde, cuando el primer receptor de comunicador recibe la primera secuencia de números dentro del área vallada geográficamente, el primer motor criptográfico de comunicador puede crear la clave criptográfica; y
en donde, cuando el primer receptor de comunicador está fuera del área vallada geográficamente, el primer motor criptográfico de comunicador no puede crear la clave criptográfica.

2. El sistema de la reivindicación 1, en donde el dispositivo comprende adicionalmente:

un receptor configurado para recibir una segunda secuencia de números aleatorios; y
un procesador configurado para integrar la segunda secuencia de números aleatorios en la primera secuencia de números aleatorios para formar una secuencia combinada; en donde el transmisor está configurado para transmitir la secuencia combinada.

3. El sistema de la reivindicación 1, en donde la segunda secuencia de números se recibe de un segundo generador de números aleatorios.

4. El sistema de la reivindicación 1,
en donde el primer receptor de comunicador está configurado para recibir una segunda secuencia de números desde un segundo generador de números aleatorios; en donde la memoria no transitoria está configurada para almacenar al menos una porción de la segunda secuencia; y en donde el primer procesador de comunicador está configurado para leer al menos una porción de la segunda secuencia y usa ambas de las porciones de la primera y la segunda secuencias para crear la clave criptográfica.

5. Un método para encriptar y desencriptar datos, comprendiendo el método:

definir, usando una colección de transmisores (100A, 100B, 100C), un área vallada geográficamente basándose en un alcance de señal del transmisor;
generar una pluralidad de secuencias de números aleatorios (102A, 102B, 102C) usando una pluralidad de generadores de números aleatorios;
transmitir, por cada transmisor, una de las secuencias de números dentro del área vallada geográficamente;
permitir que un primer comunicador (103) acceda a datos dentro del área vallada geográficamente, al:

recibir, en el primer comunicador, una primera secuencia;
almacenar, en una memoria no transitoria del primer comunicador, al menos una porción de la primera secuencia;
convertir, usando un procesador del primer comunicador, la porción de la primera secuencia en una clave criptográfica usando un algoritmo, en donde la clave criptográfica a partir de la primera secuencia se crea para desencriptar datos en el área vallada geográficamente; y
denegar al primer comunicador el acceso a los datos dentro del área vallada geográficamente al no recibir la primera secuencia en el primer comunicador.

6. El método de la reivindicación 5, que comprende adicionalmente:

recibir, en un receptor, una segunda secuencia de números;
combinar, usando un procesador, la primera secuencia con la segunda secuencia para formar una secuencia combinada; y
transmitir la secuencia combinada con el transmisor.

7. El método de la reivindicación 5, que comprende adicionalmente:

recibir, en un primer comunicador, una segunda secuencia de números generada por un segundo generador de números aleatorios;
almacenar, en una memoria no transitoria del primer comunicador, al menos una porción de la segunda secuencia; y
convertir, usando un procesador del primer comunicador, la porción de la primera y la segunda secuencias en una clave criptográfica usando un algoritmo.

Figura 1

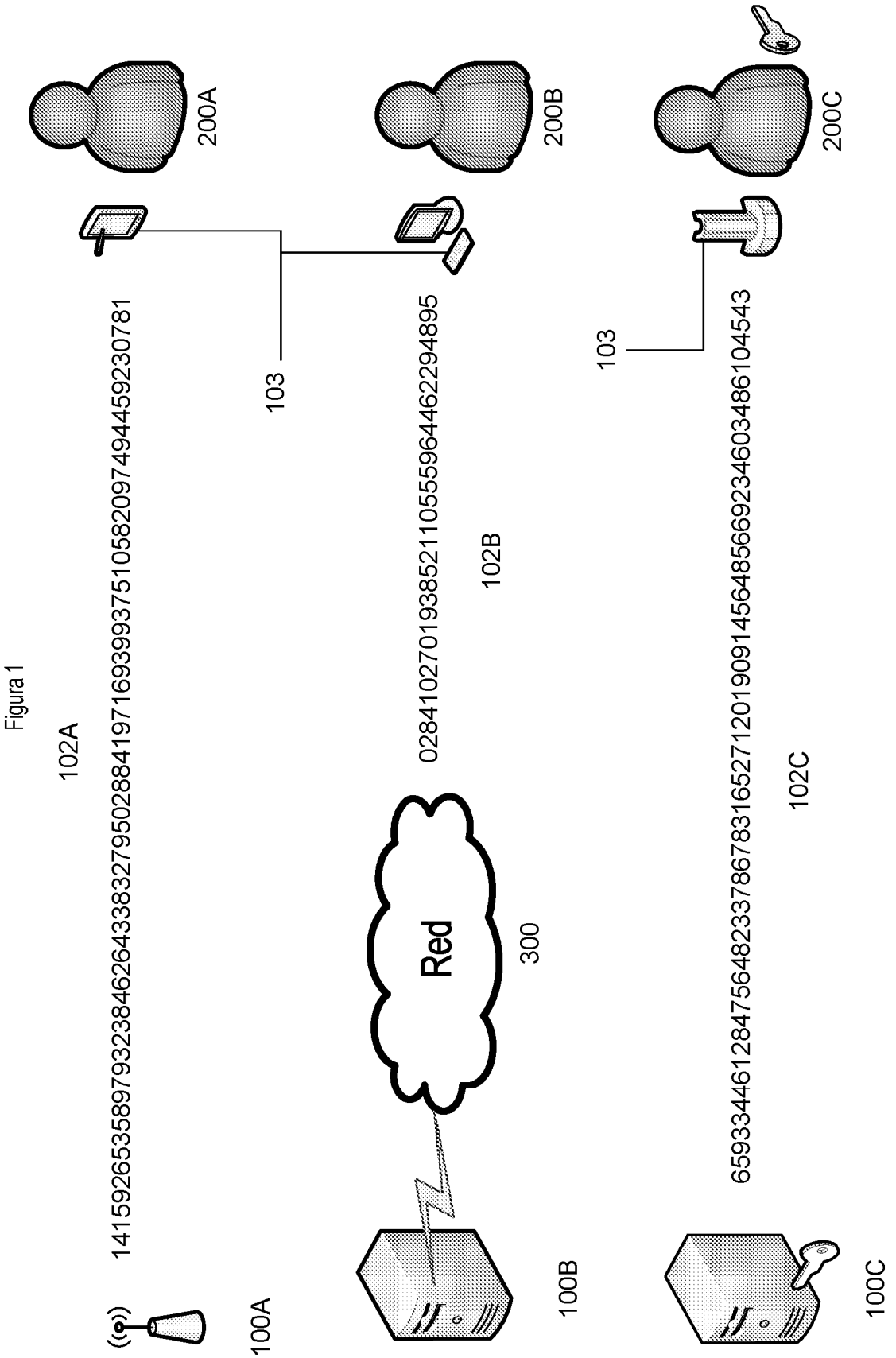
102A
14159265358979323846264338327950288419716939937510582097494459230781
100A
Red
300
100B
103
200A
200B
0284102701938521105559644622948 95
102B
103
200C
659334461284756482337867831652712019091456485669234603486104543
102C
100C

Figura 2

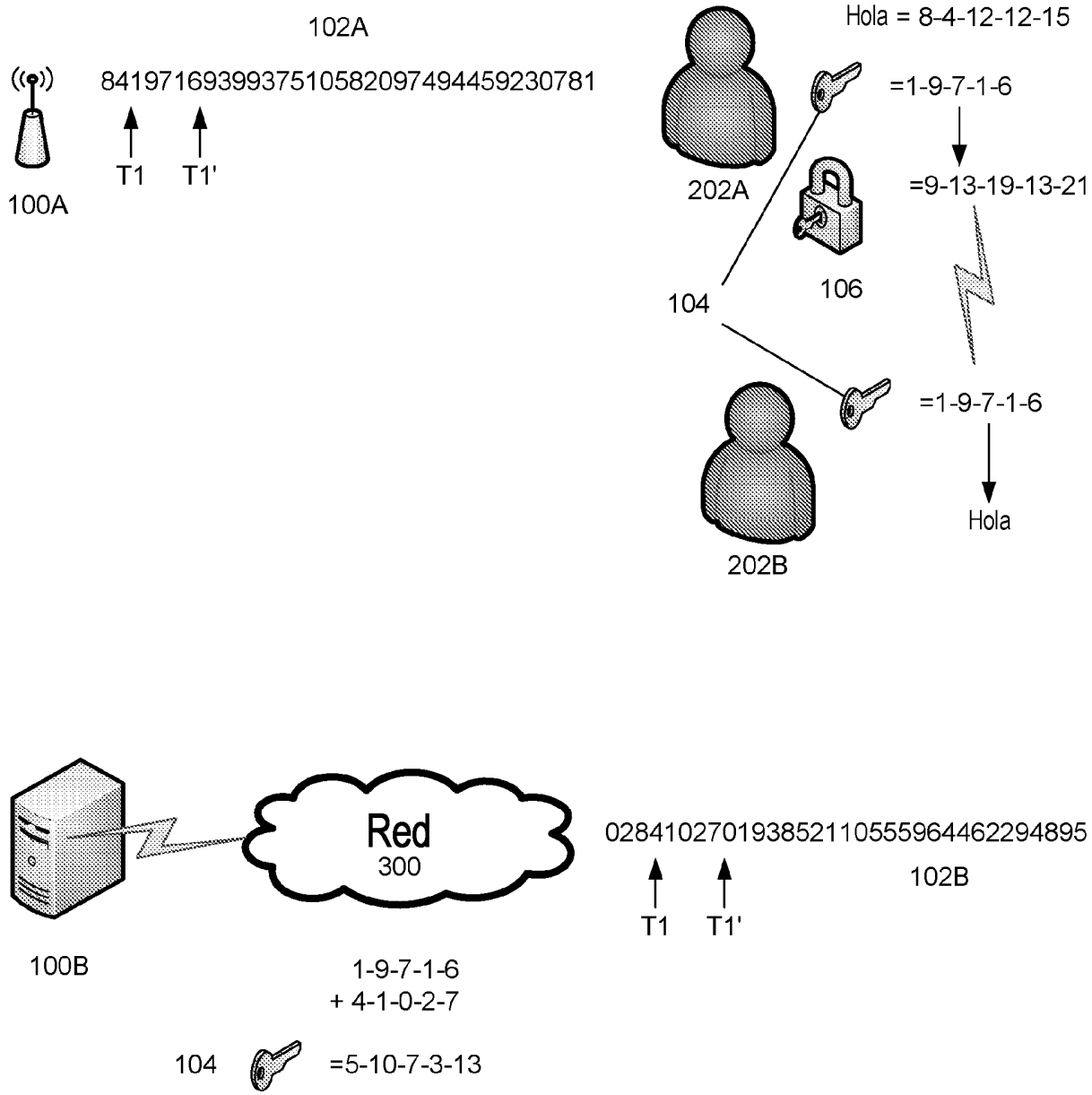
102A
841971693993751058209749445923078 1
T1
T1'
100A
Hola = 8-4-12-12-15
=1-9-7-1-6
=9-13-19-13-21
202A
106
104
=1-9-7-1-6
Hola
202B
Red
300
028410270193852110555964462294895
102B
T1
T1'
100B
1-9-7-1-6
+ 4-1-0-2-7
104
=5-10-7-3-13

Figura 3

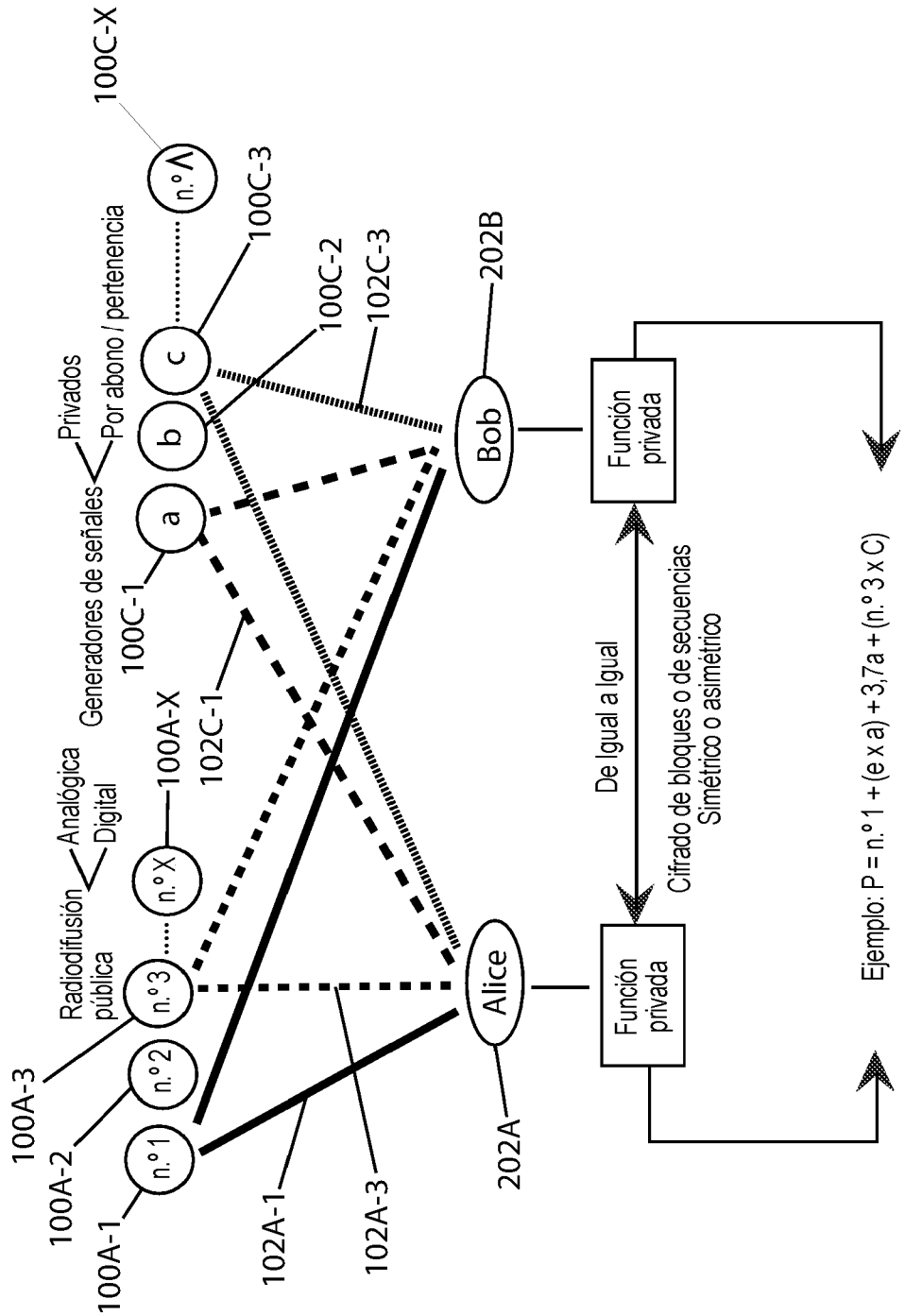
Radiodifusión pública
Analógica
Digital
Generadores de señales
Privados
Por abono / pertenencia
100A-3
100A-2
100A-1
100A-X
100C-1
100C-2
100C-3
100C-X
102C-1
102C-3
102A-1
102A-3
202A
202B
Alice
Bob
n.º 1
n.º 2
n.º 3
n.º X
n.º Y
a
b
c
Función privada
Función privada
De igual a igual
Cifrado de bloques o de secuencias
Simétrico o asimétrico
Ejemplo: P = n.º 1 + (e x a) + 3,7a + (n.º 3 x C)

Figura 4

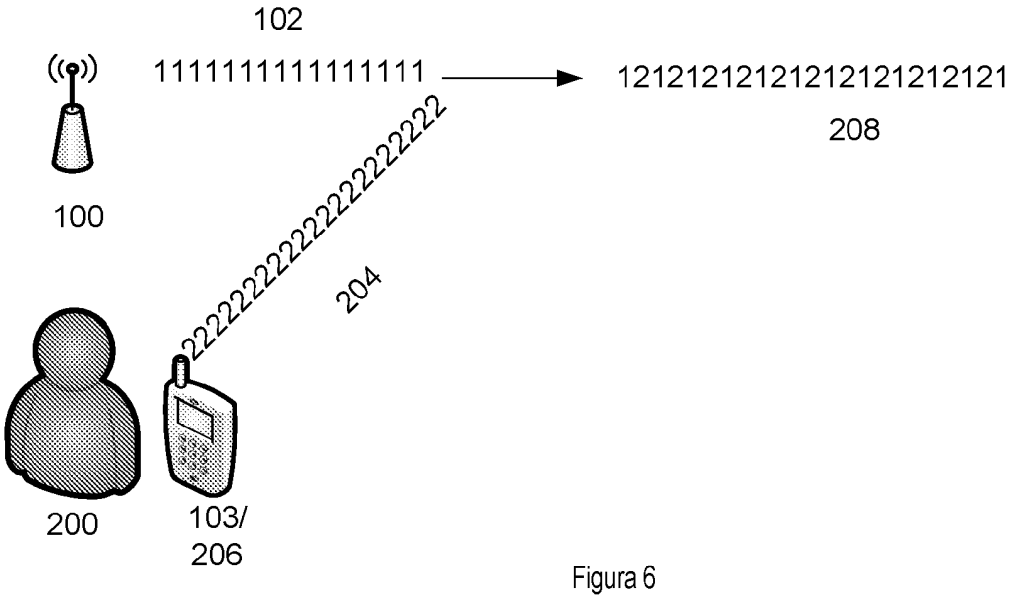

Figura 6

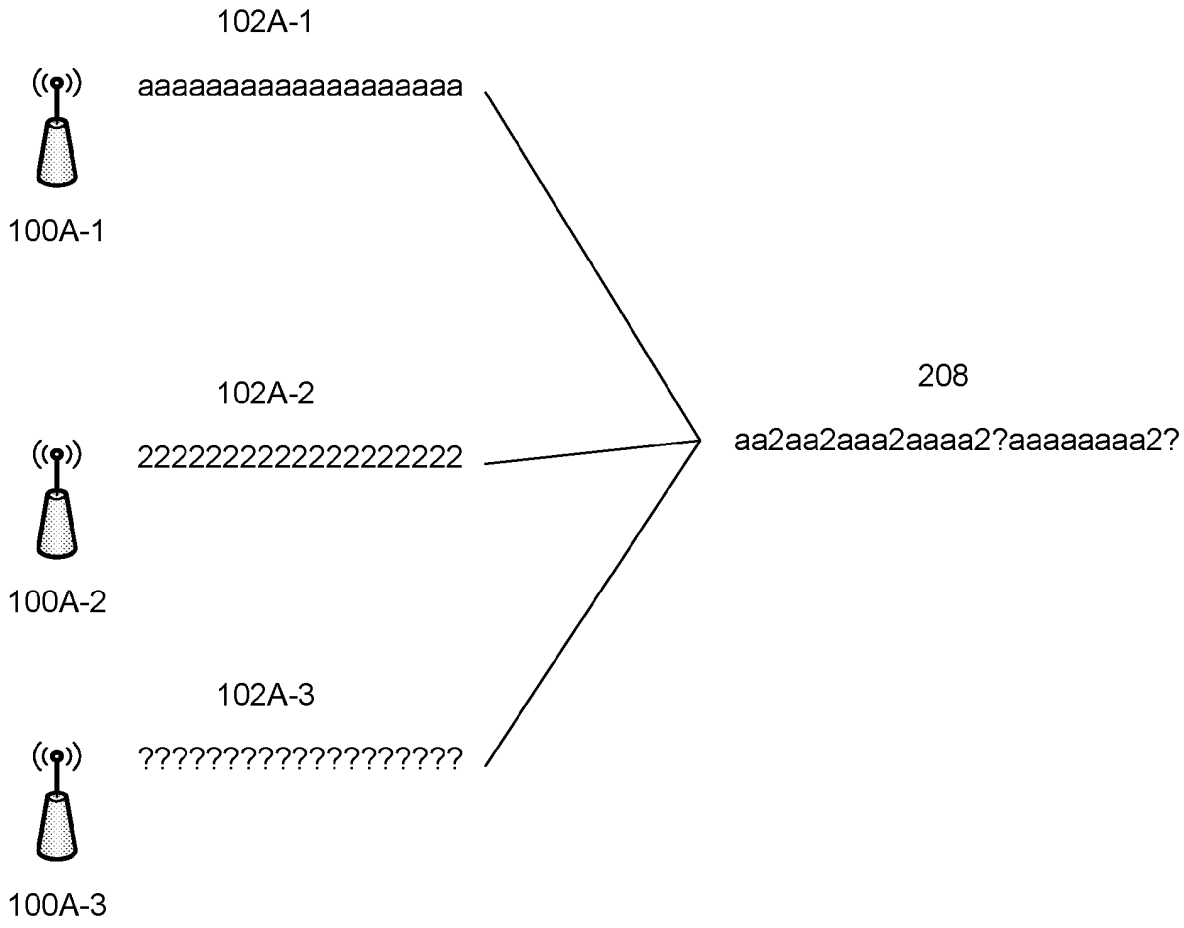

Figura 5

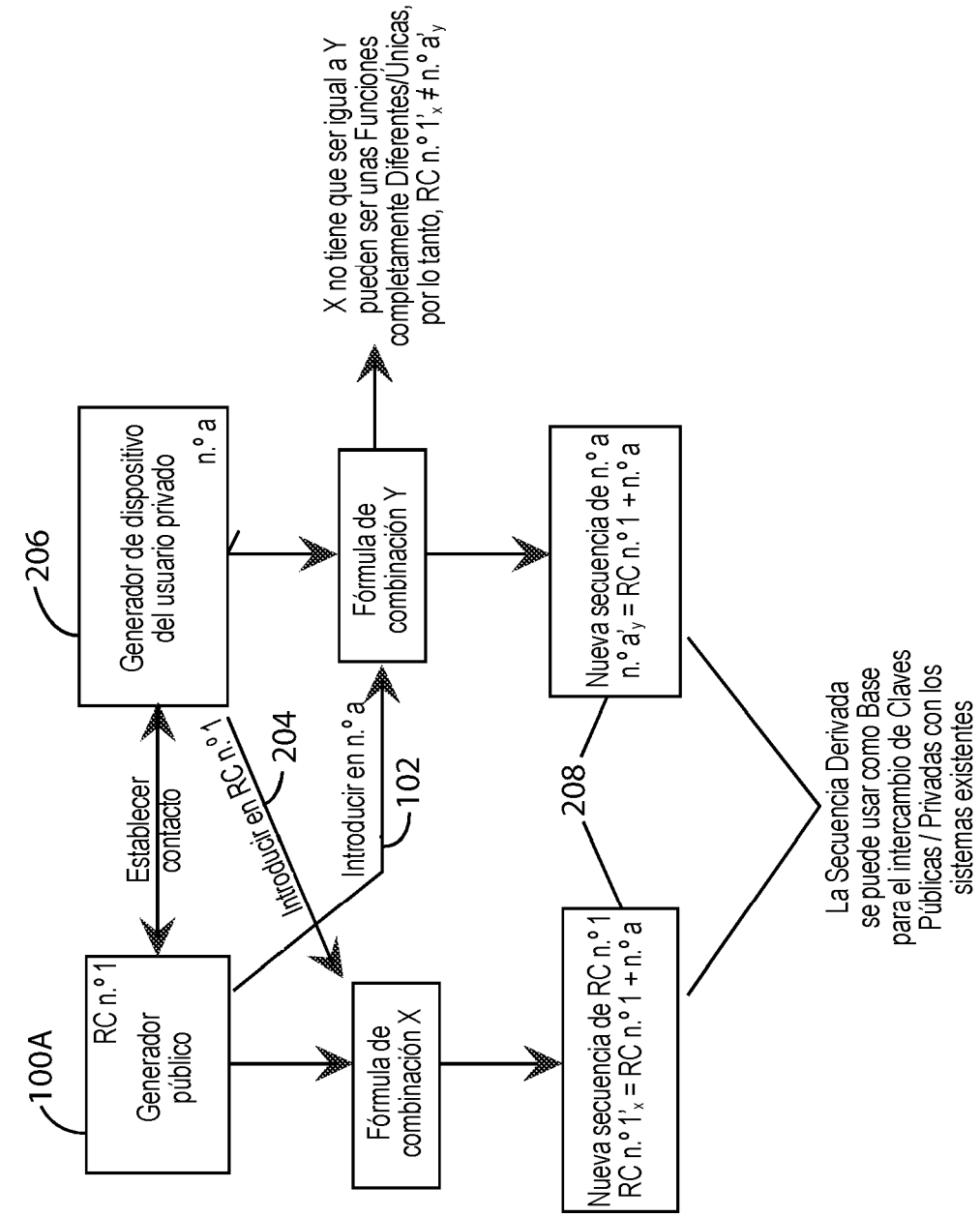
100A
RC n.º 1
Generador público
206
Generador de dispositivo del usuario privado n.º a
Establecer contacto
Introducir en RC n.º 1
204
Introducir en n.º a
102
Fórmula de combinación X
Fórmula de combinación Y
X no tiene que ser igual a Y pueden ser unas Funciones completamente Diferentes/Unicas, por lo tanto, RC n.º 1'x ≠ n.º a'y
Nueva secuencia de RC n.º 1 RC n.º 1'x = RC n.º 1 + n.º a
208
Nueva secuencia de n.º a n.º a'y = RC n.º 1 + n.º a
La Secuencia Derivada se puede usar como Base para el intercambio de Claves Públicas / Privadas con los sistemas existentes

Figura 7

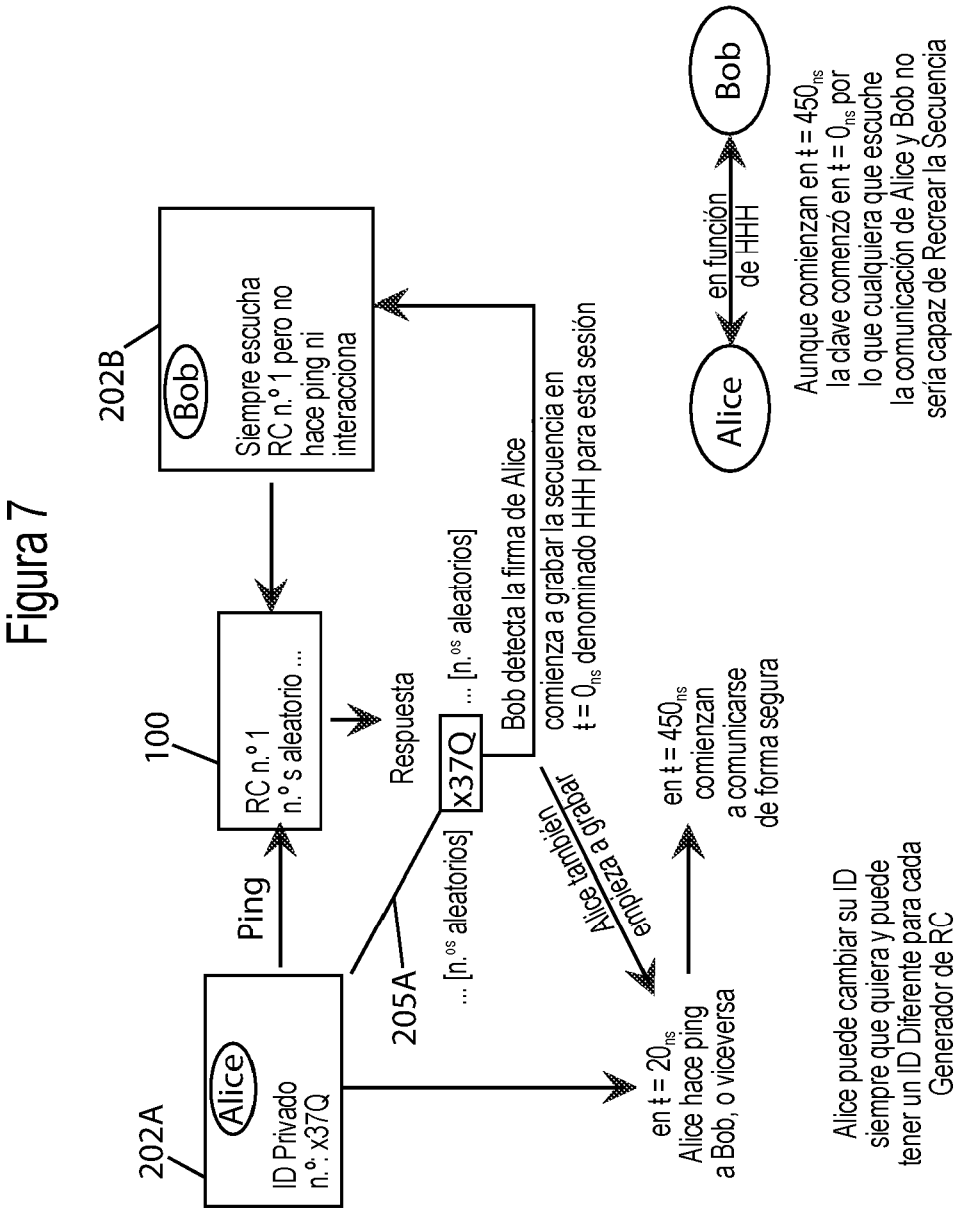
202A
Alice
ID Privado
n.º: x37Q
Ping
100
RC n.º 1
n.º s aleatorio ...
Respuesta
202B
Bob
Siempre escucha
RC n.º 1 pero no
hace ping ni
interacciona
205A
... [n.os aleatorios]
x37Q
... [n.os aleatorios]
Bob detecta la firma de Alice
comienza a grabar la secuencia en
t = 0ns denominado HHH para esta sesión
Alice también
empieza a grabar
en t = 20ns
Alice hace ping
a Bob, o viceversa
en t = 450ns
comienzan
a comunicarse
de forma segura
Alice puede cambiar su ID
siempre que quiera y puede
tener un ID Diferente para cada
Generador de RC
Alice
en función
de HHH
Bob
Aunque comienzan en t = 450ns
la clave comenzó en t = 0ns por
lo que cualquiera que escuche
la comunicación de Alice y Bob no
sería capaz de Recrear la Secuencia

Figura 8

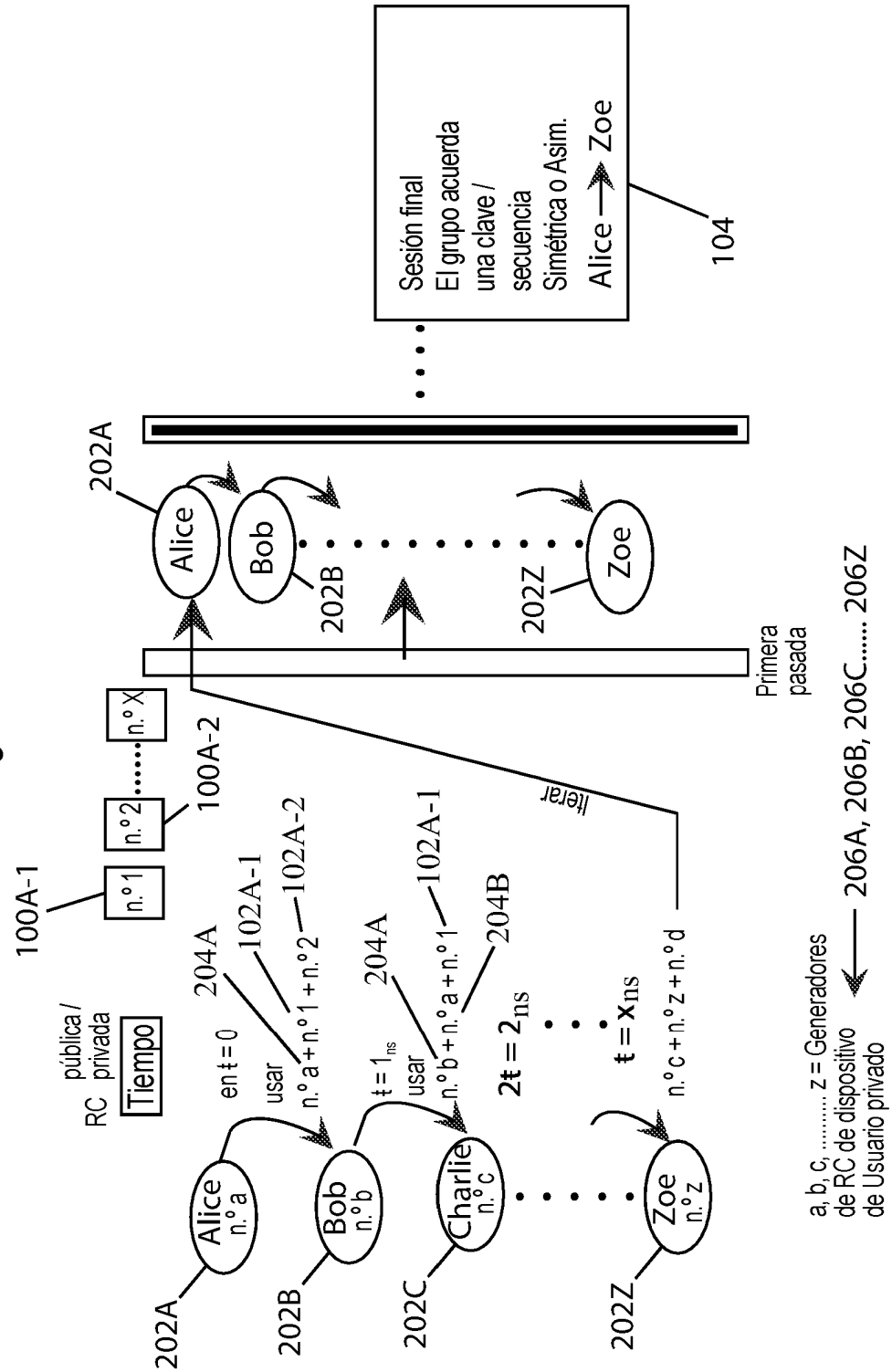
100A-1
n.º 1
n.º 2
n.º X
100A-2
RC pública / privada
Tiempo
202A
Alice
202B
Bob
202C
Charlie
n.º c
202Z
Zoe
n.º z
204A
en t = 0
usar
n.º a + n.º 1 + n.º 2
102A-1
102A-2
t = 1ns
usar
n.º b + n.º a + n.º 1
204B
2t = 2ns
t = xns
n.º c + n.º z + n.º d
Iterar
Primera pasada
Sesión final
El grupo acuerda una clave / secuencia
Simétrica o Asim.
Alice → Zoe
104
a, b, c, ... z = Generadores de RC de dispositivo de Usuario privado
206A, 206B, 206C..... 206Z

Figura 9

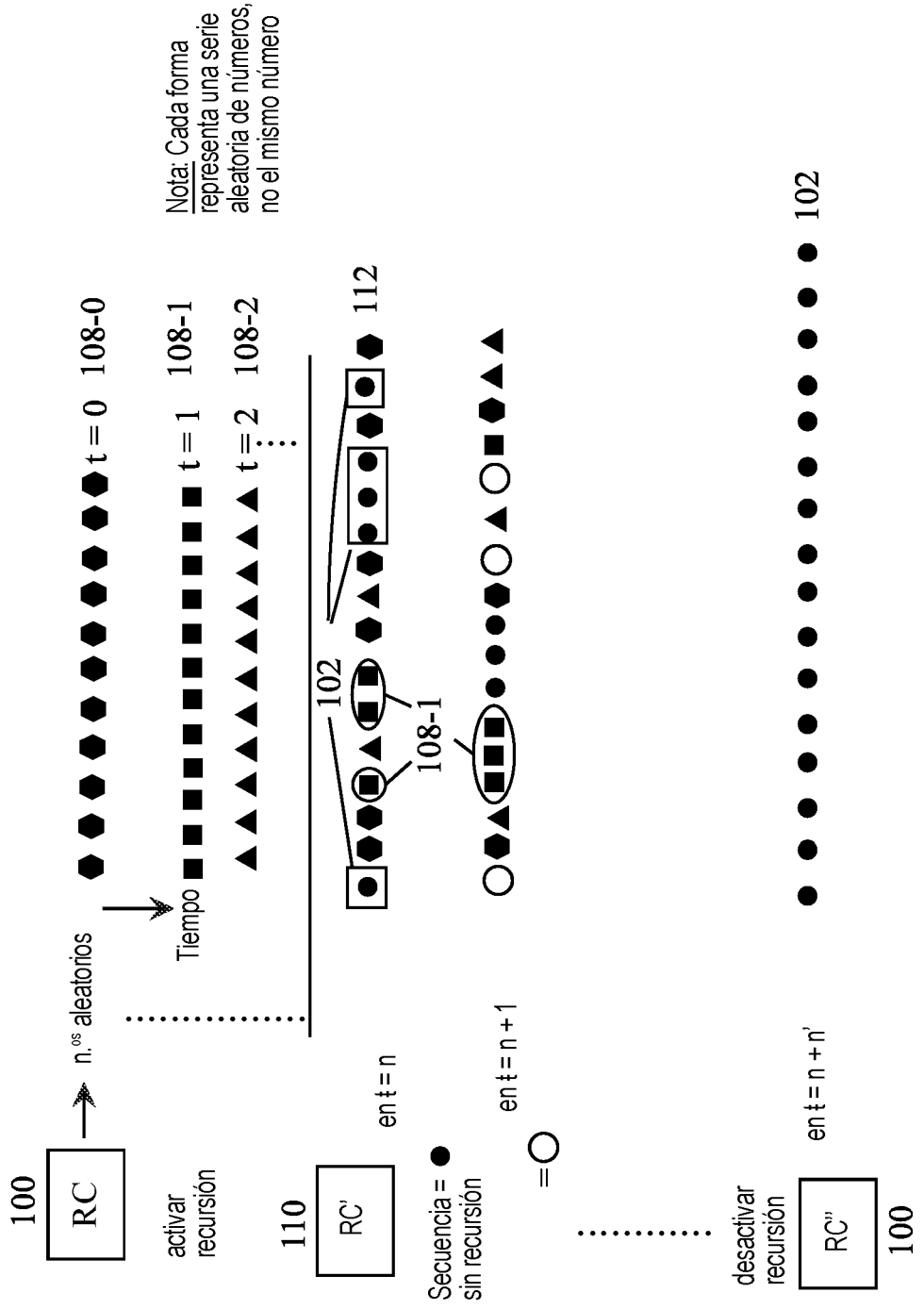
100
RC
n.os aleatorios
activar recursión
Tiempo
t = 0
108-0
t = 1
108-1
t = 2
108-2
Nota: Cada forma representa una serie aleatoria de números, no el mismo número
110
RC'
en t = n
102
108-1
112
Secuencia = sin recursión
en t = n + 1
=
desactivar recursión
RC''
en t = n + n'
102
100

Figura 10

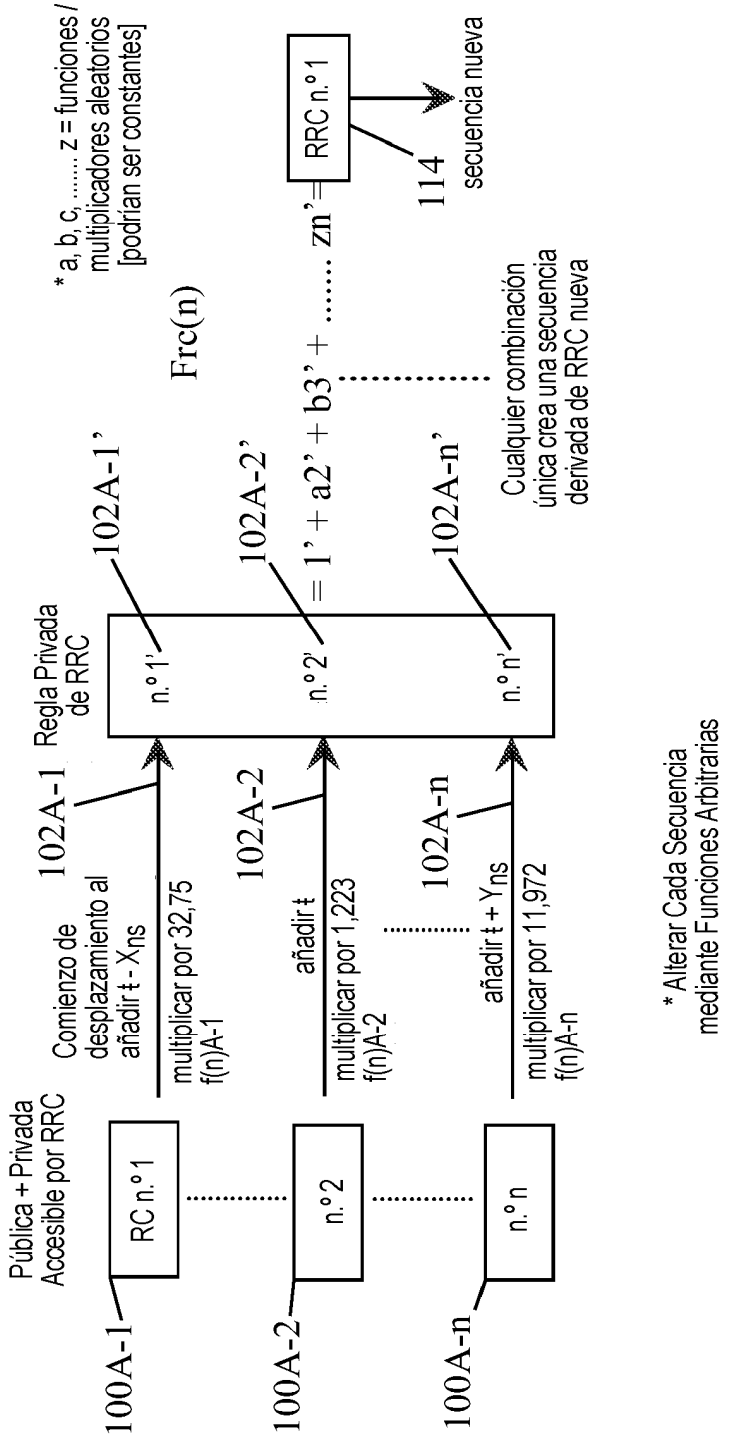
Pública + Privada
Accesible por RRC
RC n.º 1
n.º 2
n.º n
100A-1
100A-2
100A-n
Comienzo de desplazamiento al añadir t - Xns
multiplicar por 32,75
f(n)A-1
102A-1
Regla Privada de RRC
añadir t
multiplicar por 1,223
f(n)A-2
102A-2
añadir t + Yns
multiplicar por 11,972
f(n)A-n
102A-n
n.º 1'
n.º 2'
n.º n'
102A-1'
102A-2'
102A-n'
Frc(n)
= 1' + a2' + b3' + ... zn'=
* a, b, c, ... z = funciones / multiplicadores aleatorios [podrían ser constantes]
RRC n.º 1
114
secuencia nueva
Cualquier combinación única crea una secuencia derivada de RRC nueva
* Alterar Cada Secuencia mediante Funciones Arbitrarias

Figura 11

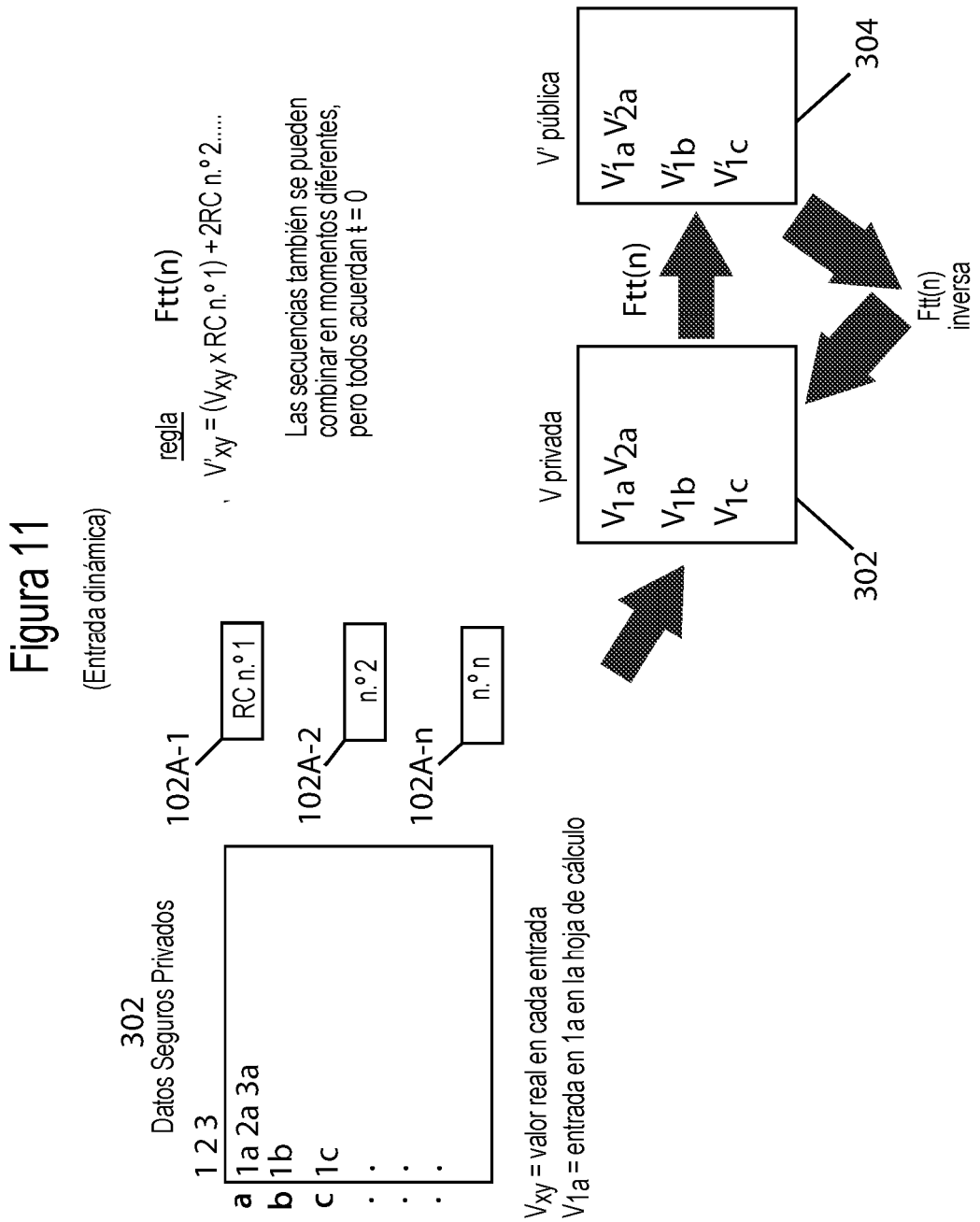
(Entrada dinámica)
302
Datos Seguros Privados
1 2 3
a 1a 2a 3a
b 1b
c 1c
. . .
. . .
. . .
102A-1
RC n.º 1
102A-2
n.º 2
102A-n
n.º n
Vxy = valor real en cada entrada
V1a = entrada en 1a en la hoja de cálculo
regla
Ftt(n)
V'xy = (Vxy x RC n.º 1) + 2RC n.º 2.....
Las secuencias también se pueden combinar en momentos diferentes, pero todos acuerdan t = 0
V privada
V1a V2a
V1b
V1c
Ftt(n)
V' pública
V'1a V'2a
V'1b
V'1c
304
302
Ftt(n) inversa

Figura 12A

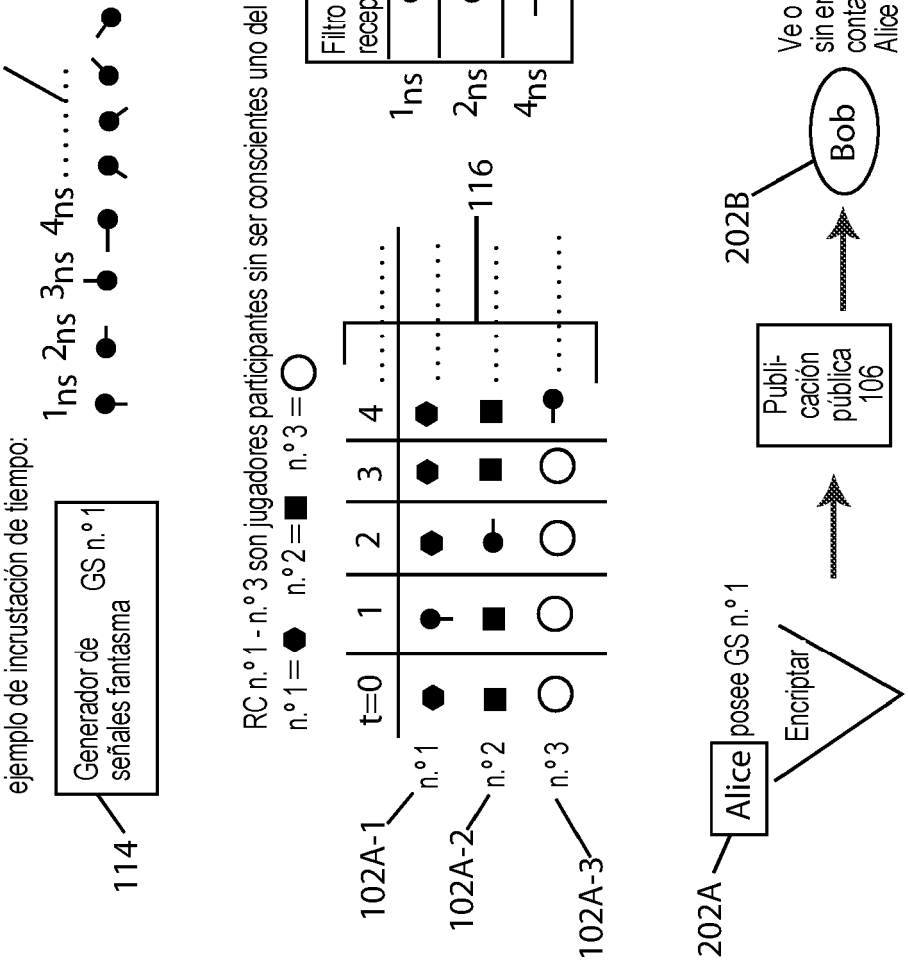
ejemplo de incrustación de tiempo:
Generador de señales fantasma
GS n.º 1
114
212
1ns 2ns 3ns 4ns
RC n.º 1 - n.º 3 son jugadores participantes sin ser conscientes uno del otro. Añaden GS n.º 1 en t = 1ns 2ns 3ns 4ns
n.º 1 = n.º 2 = n.º 3 =
t=0 1 2 3 4
n.º 1
n.º 2
n.º 3
102A-1
102A-2
102A-3
116
Filtro de receptor
214
1ns
2ns
4ns
Recrear la GS n.º 1 sin nunca acoplarse o escuchar directamente la señal de GS n.º 1
202A
Alice
posee GS n.º 1
Encriptar
Mensaje
Publi-cación pública 106
202B
Bob
Ve o descarga sin entrar en contacto con Alice
214
Aplica filtro de GS n.º 1
Texto sin formato

Figura 12B

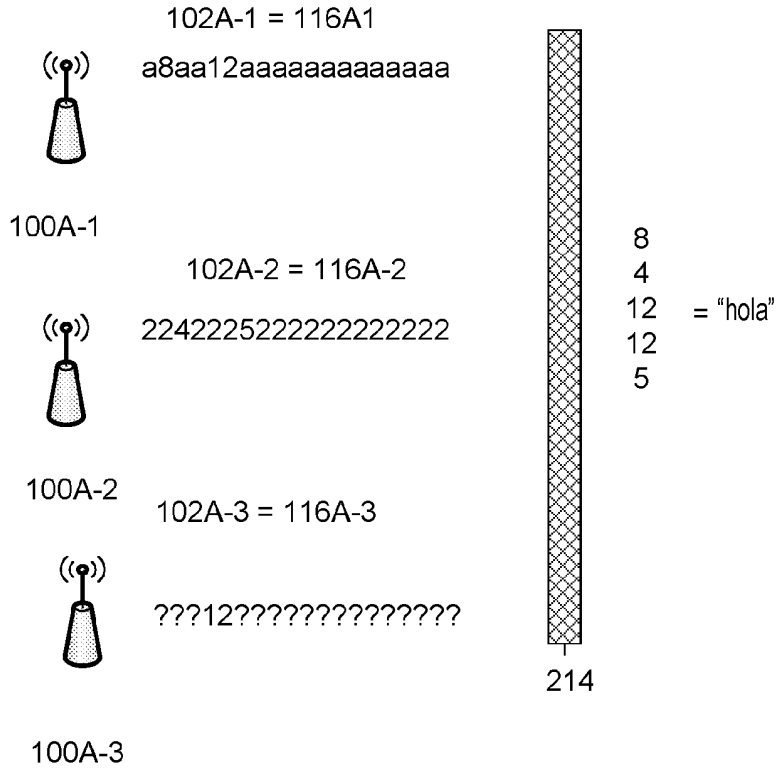

Figura 14

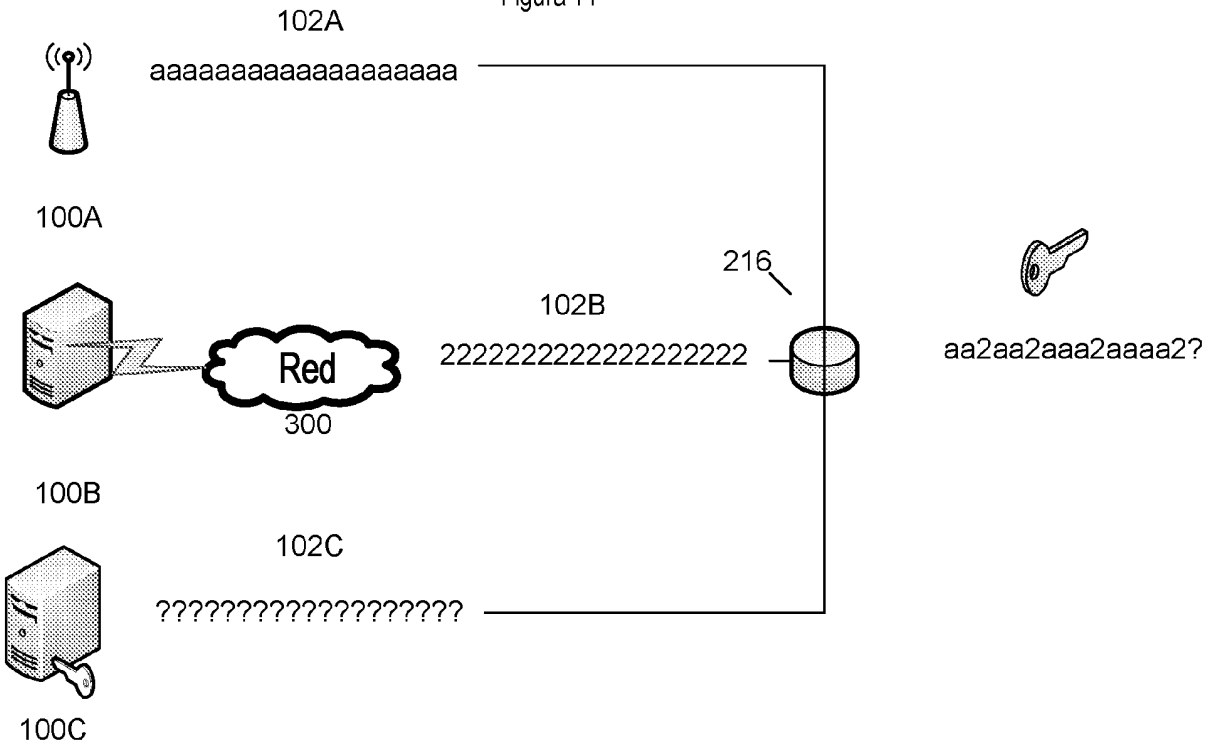

Figura 13

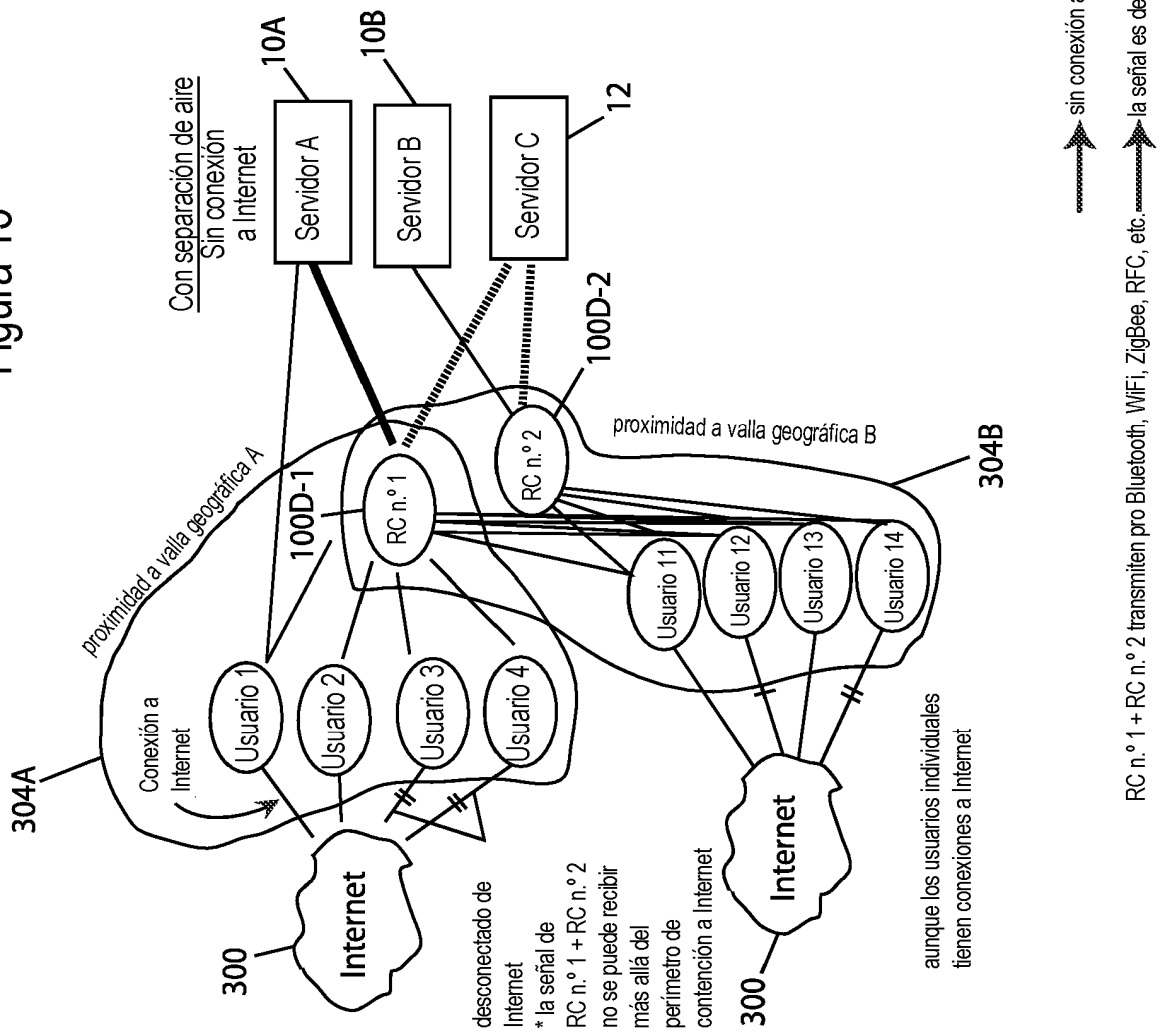
Los usuarios 1 - 4 solo acceden a RC n.º 1 y al servidor A cuando están dentro de la valla geográfica - el límite de la potencia de señal
Los usuarios 11 - 14 acceden a ambos de RC n.º 1 + 2 pero solo pueden usar el servidor B
1 - 4, 11, 14 pueden acceder, todos ellos, al centro de datos
* No hay forma alguna de que un extraño acepte la señal sin tener un sensor en la Valla geográfica
Con separación de aire
Sin conexión a Internet
10A
10B
12
Servidor A
Servidor B
Servidor C
100D-1
100D-2
RC n.º 1
RC n.º 2
proximidad a valla geográfica A
proximidad a valla geográfica B
304A
304B
300
300
Conexión a Internet
Internet
Internet
Usuario 1
Usuario 2
Usuario 3
Usuario 4
Usuario 11
Usuario 12
Usuario 13
Usuario 14
desconectado de Internet
* la señal de RC n.º 1 + RC n.º 2 no se puede recibir más allá del perímetro de contención a Internet
aunque los usuarios individuales tienen conexiones a Internet
sin conexión a Internet
la señal es de muy corto alcance
RC n.º 1 + RC n.º 2 transmiten pro Bluetooth, WiFi, ZigBee, RFC, etc.

Figura 15

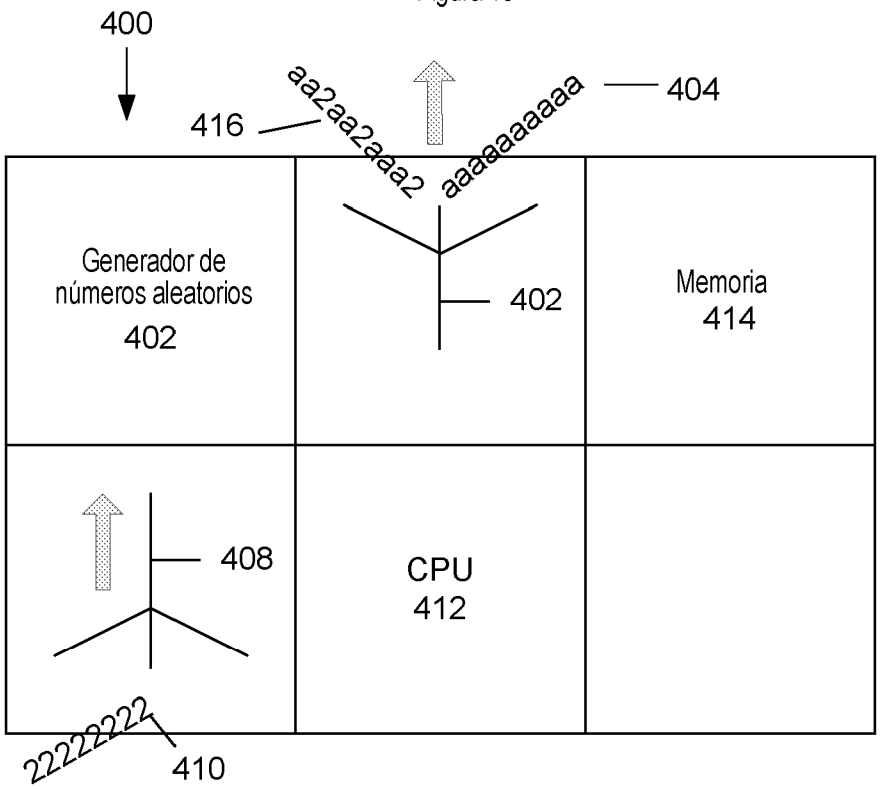

Figura 16

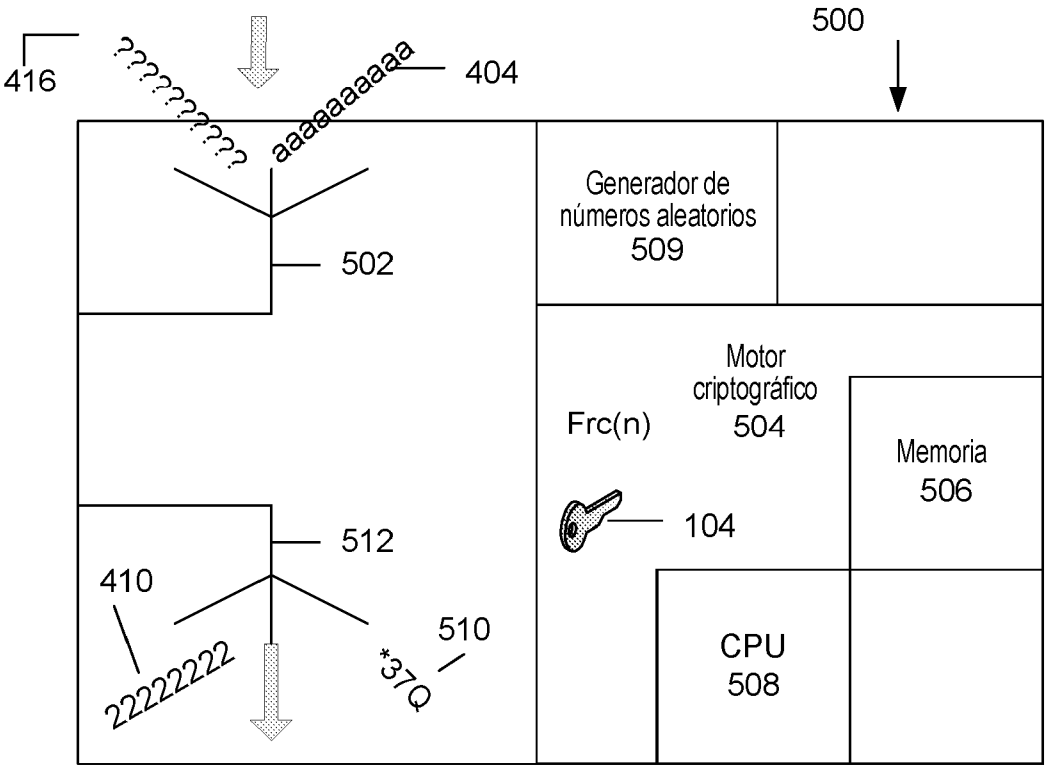

Figura 17

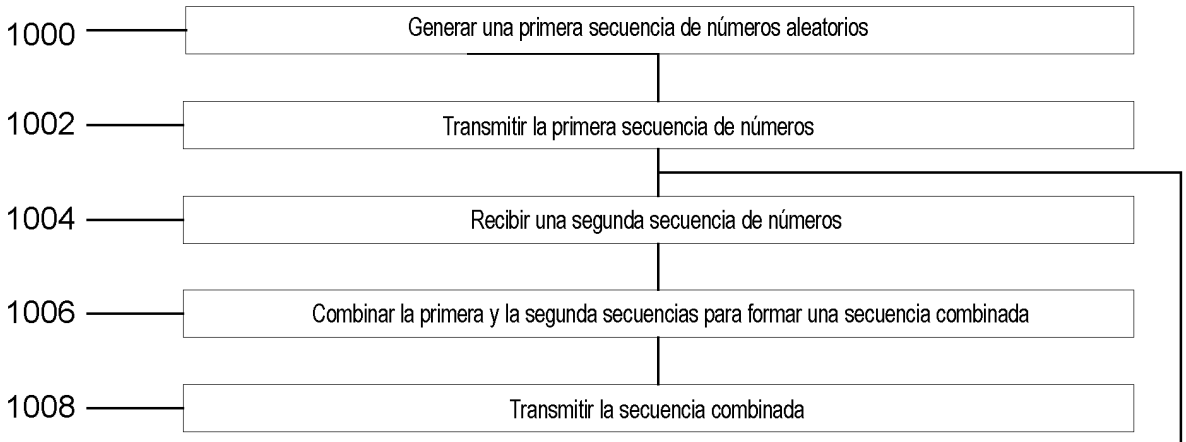

Figura 18

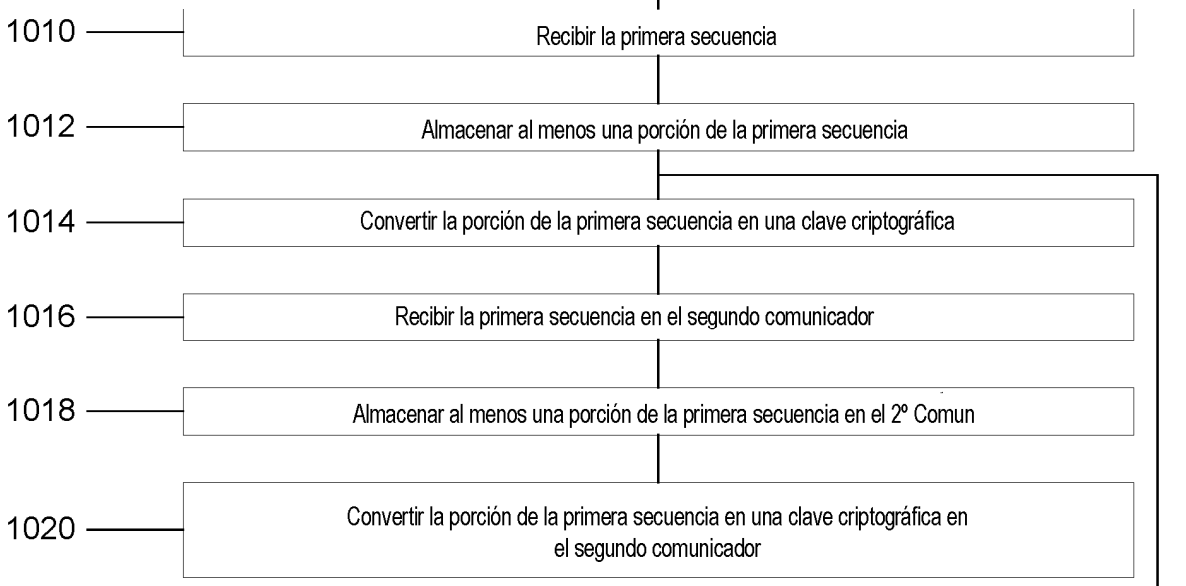

Figura 19

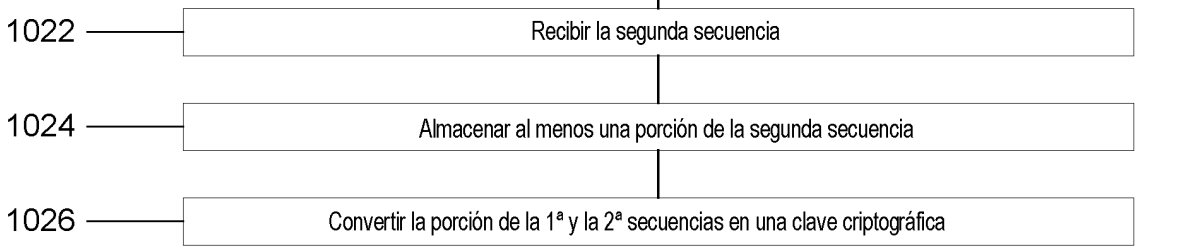

Figura 20

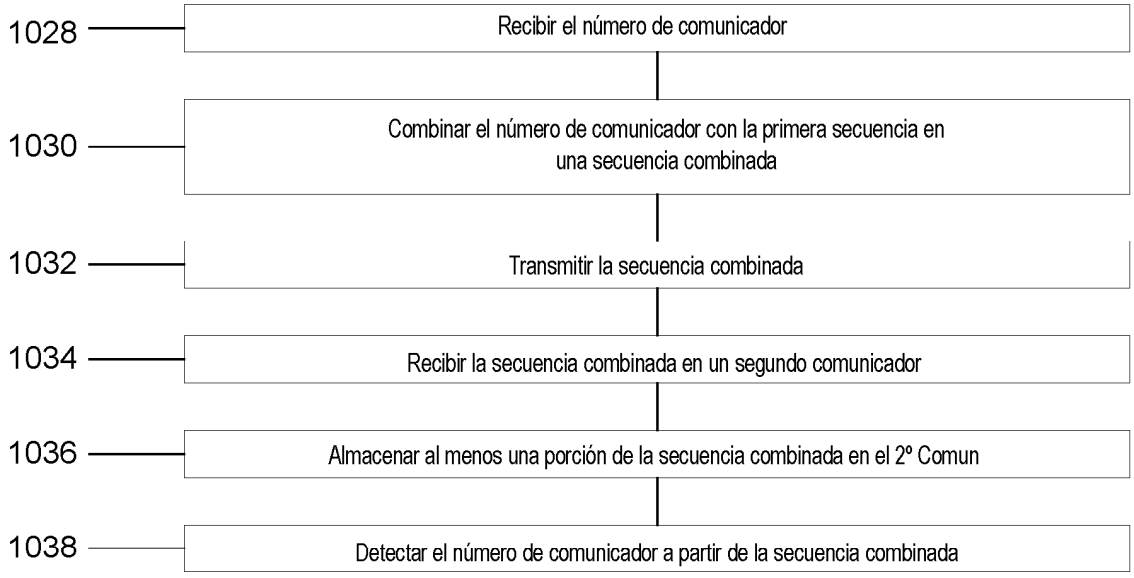

Figura 21

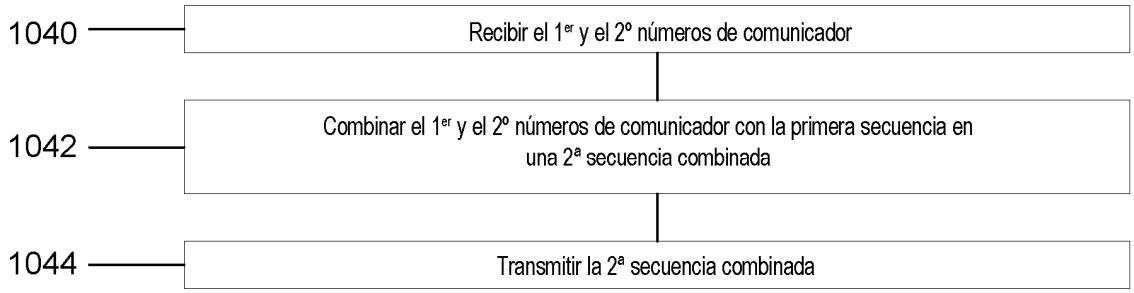

Figura 22

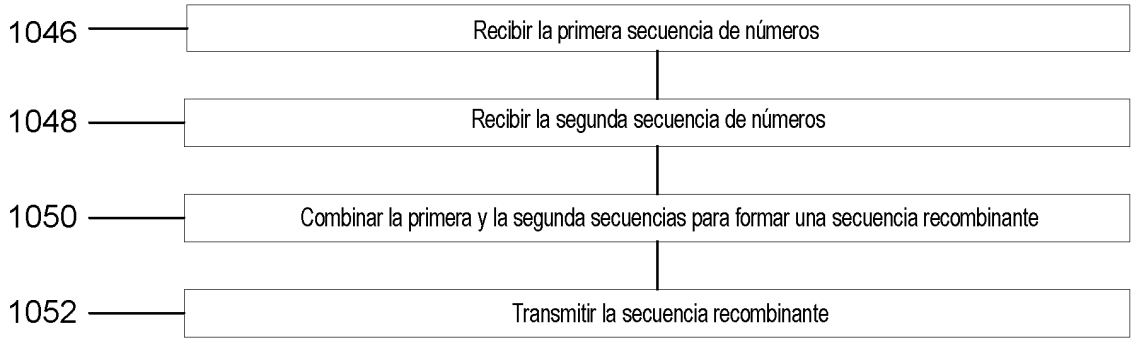

Figura 23

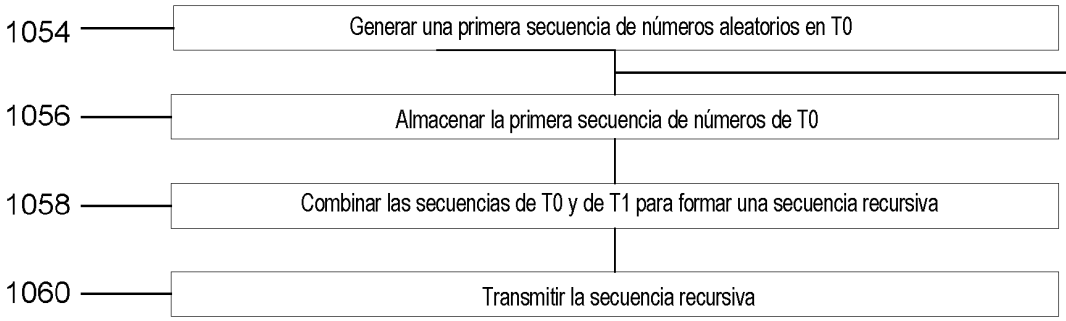

Figura 24

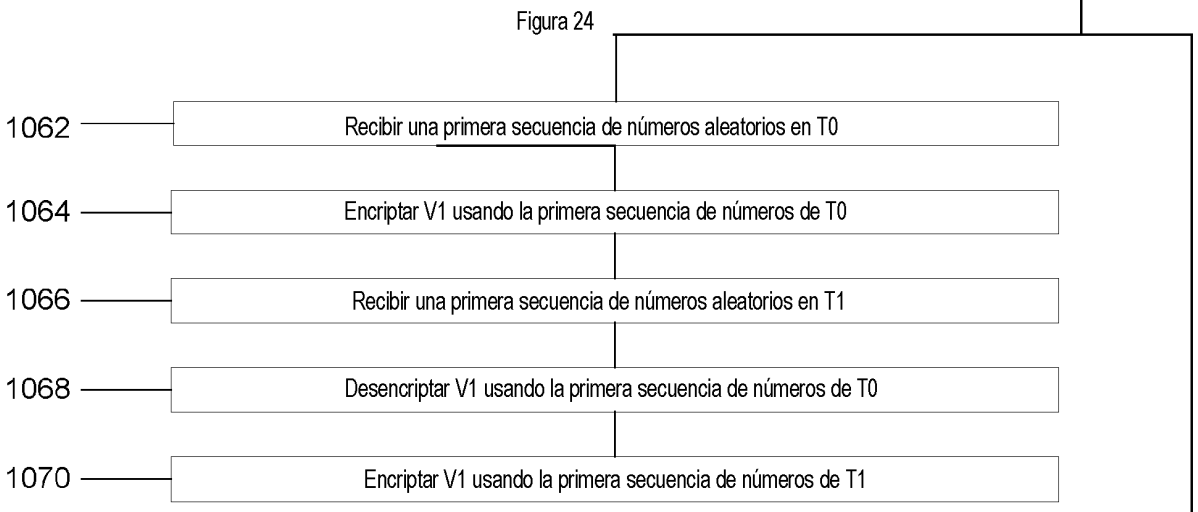

Figura 25

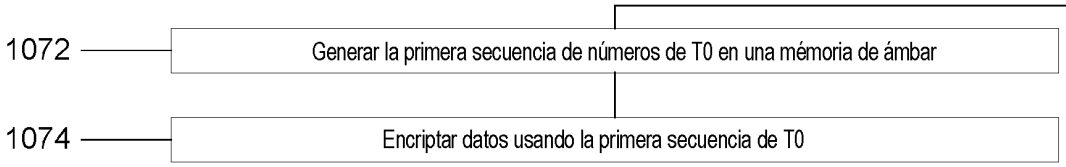

Figura 26

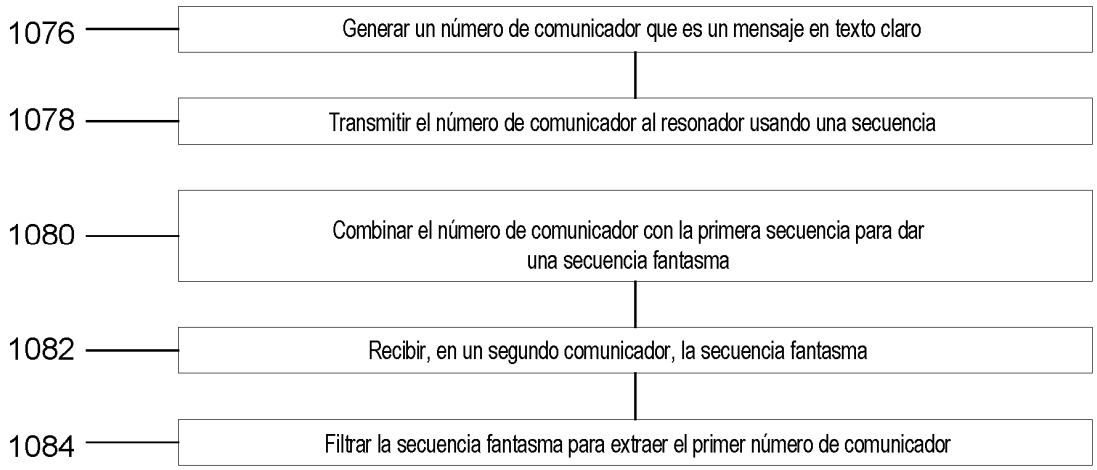

Figura 27