(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 763 079**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.12.2016 PCT/EP2016/082874**

(87) Fecha y número de publicación internacional: **06.07.2017 WO17114920**

(96) Fecha de presentación y número de la solicitud europea: **29.12.2016 E 16831622 (2)**

(97) Fecha y número de publicación de la concesión europea: **18.09.2019 EP 3398290**

(54) Título: **Procedimiento de extracción univalente y unívoca de claves a partir del canal de propagación**

(30) Prioridad:

29.12.2015 FR 1502712

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.05.2020

(73) Titular/es:

THALES (33.3%)
Tour Carpe Diem, Place des Corolles, Esplanade Nord
92400 Courbevoie, FR;
INSTITUT MINES-TÉLÉCOM (33.3%) y
CELENO COMMUNICATIONS LTD. (33.3%)

(72) Inventor/es:

MOLIÈRE, RENAUD;
KAMENI NGASSA, CHRISTIANE;
DELAVEAU, FRANÇOIS;
LEMÉNAGER, CLAUDE;
SIBILLE, ALAIN;
MAZLOUM, TAGHRID y
SHAPIRA, NIR

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de extracción univalente y unívoca de claves a partir del canal de propagación

La invención se refiere a un procedimiento de extracción univalente y unívoca de claves a partir del canal de propagación. Estas claves, convertidas en secretas debido a la univalencia del procedimiento, están destinadas a ser utilizadas para asegurar el intercambio de datos entre al menos un primer usuario y al menos un segundo usuario, en un sistema de intercambio de datos, en concreto sistemas de comunicaciones inalámbricas (terminales portátiles, ordenadores, etc.).

Para los intercambios de datos, en concreto en los sistemas de comunicaciones inalámbricas, es preferible asegurar la información transmitida entre dos usuarios, para evitar que un tercero malintencionado acceda a esta información.

La mayor parte de los sistemas de transmisión seguros utilizan claves secretas compartidas previamente entre los emisores y los receptores, lo que induce mecanismos complejos (y a menudo costosos) de generación y de distribución de dichas claves para compartirlas entre los usuarios. Además, cuando esta generación y esta distribución deben efectuarse a gran escala, como por ejemplo en las redes de radiocomunicaciones públicas, la multiplicación de los participantes (fabricantes, operadores, distribuidores, abonados) y de los circuitos de encauzamiento inducen fuertes riesgos de fuga de datos, como han demostrado varios hechos diversos en el campo.

Existen ciertos dispositivos de generación de claves secretas a partir del canal de propagación. Estos dispositivos utilizan la indicación de la intensidad de la señal recibida (RSSI). En términos tecnológicos, esta medida de potencia es de acceso bastante fácil. Sin embargo, el RSSI solamente tiene en cuenta una pequeña parte de la riqueza del canal de propagación, ignorando los coeficientes de fase de canal que ofrecen mucho más carácter aleatorio que el único parámetro de potencia de la señal habitualmente aprovechada. Debido a esto, en situaciones frecuentes, la generación de clave por aprovechamiento del RSSI no es univalente ya que las claves generadas presentan fuertes correlaciones, lo que permite a un tercero reconstituirlas. El artículo "Applying Beamforming to Address Temporal Correlation in Wireless Channel Characterization-Based Secret Key Generation" de M. Madiseh et al., publicado en "IEEE transactions of Information Forensics and Security", vol. 7, no. 4, agosto de 2012, expone un procedimiento de generación de claves implementado por dos dispositivos de comunicación inalámbrica sobre la base de un análisis de la respuesta impulsional del canal.

El artículo "The Generation of Shared Cryptographic Keys through Full Duplex Channel Impulse Response Estimation at 60 GHz" de M. Forman y D. Young, publicado en "Proceedings of Asia Microwave Conference 2010", expone un dispositivo de comunicación inalámbrica que genera una clave sobre la base de un análisis de la respuesta impulsional del canal.

Los documentos de publicación de solicitud de patente US 2012/0281834 A1 de Reznik et al, y WO 2006/081122 A2 de Rudolf et al, exponen técnicas relevantes para los antecedentes tecnológicos en el que se sitúa la presente invención.

La idea implementada por el procedimiento según la invención es, en concreto, aprovechar plenamente el carácter fuertemente aleatorio de los canales de transmisión inalámbrica, para generar de forma univalente y unívoca una clave secreta que permita la protección de los datos intercambiados entre al menos un emisor y un receptor. Proviniendo dicha univalencia del hecho de que una sola medida de la canal realizada de manera simultánea y colocalizada permitiría a un tercero no informado de dichas medidas, reproducir estas claves aplicando los mismos procedimientos de selección, cuantificación y formateo; dicha univocidad proviene de los mecanismos de formateo y de corrección aplicados en el procedimiento según la invención.

En lo sucesivo en la descripción, se utiliza indistintamente la expresión "usuario A" o "emisor receptor A" para designar un usuario Alice y del mismo modo para el usuario Bob.

La invención se refiere a un procedimiento de extracción univalente y unívoca de claves a partir de un canal de propagación (EUC_CP), estando dichas claves destinadas a proteger datos intercambiados entre un primer usuario y un segundo usuario, constando un usuario de uno o varios emisores y uno o varios receptores, siendo los datos transmitidos por el canal de propagación, caracterizado porque consta al menos de las etapas siguientes:

a) Medir mediante el o los receptores del primer y del segundo usuario, señales S que provienen de cada emisor del otro usuario, medir los parámetros del canal de propagación correspondiente, y estimar las respuestas impulsionales complejas correspondientes del canal de propagación o respuestas en frecuencia complejas correspondientes del canal de propagación,

b) Seleccionar de manera univalente, para cada usuario, un conjunto de coeficientes complejos de canal resultantes de las estimaciones de las respuestas impulsionales complejas del canal de propagación o de las respuestas en frecuencia complejas del canal de propagación, y conservar los coeficientes que presentan una correlación cruzada inferior a un valor umbral predeterminado ajustable,

c) Cuantificar y formatear, para cada usuario, los coeficientes complejos de canal seleccionados, aplicando una malla geométrica del plano complejo en el que los coeficientes de canal asumen su valor, una numeración de los

coeficientes complejos según la malla a la que pertenecen, y aplicando técnicas de corrección de errores en dicha numeración,
d) Utilizar de manera univalente y unívoca, para cada usuario, datos digitales resultantes de dicha cuantificación y de dicho formateo en forma de claves secretas para encriptar la cadena de datos transmitidos.

El procedimiento utiliza, por ejemplo, como modo de comunicación entre los usuarios, un modo dúplex temporal que emplea una misma frecuencia portadora para los intercambios en emisión y en recepción en los dos sentidos de transmisión.

El procedimiento se puede duplicar en el conjunto de las frecuencias portadoras empleadas por usuarios en modo dúplex frecuencial que emplea frecuencias portadoras diferentes para sus intercambios en emisión y en recepción según el sentido de transmisión.

El procedimiento puede aplicar una función de codificación correctora de errores en las claves extraídas por los usuarios, con una transmisión mínima de datos del primer usuario hacia el segundo usuario, para eliminar las diferencias entre las claves del primer y del segundo usuario.

Según una variante de realización, el procedimiento implementa una función de troceado y una reducción de longitud en las claves extraídas, estando la función adaptada a eliminar cualquier fuga residual de información hacia un tercero y mejorar las calidades aleatorias de las claves.

Las etapas del procedimiento según la invención pueden repetirse de una transmisión a otra y repetirse regularmente durante una misma transmisión.

El procedimiento puede utilizar un protocolo de ruido y de formación de haz para la transmisión de los datos y las señales son, por ejemplo, señales emitidas y recibidas en el marco de dicho protocolo de ruido artificial y formación de haz.

Según una variante de realización, las señales son señales emitidas y recibidas en el marco de un protocolo con emisión y recepción simultáneas ("Full Duplex" en inglés).

Según otra variante, las señales son señales de marcado, públicas o no, encubiertas o no, con o sin autointerferencia, emitidas y recibidas en el marco de un protocolo de identificación de sistemas de emisión-recepción o en el marco de un protocolo de autentificación de usuarios de dicho sistema o en el marco de un protocolo de control de integridad de los mensajes emitidos y recibidos por dicho sistema.

El procedimiento puede implementar emisores y receptores adaptados a radiocomunicaciones. También puede utilizar emisores y receptores adaptados a transmisiones acústicas o también a transmisiones ópticas.

La invención también se refiere a un dispositivo que permite una extracción univalente y unívoca de claves a partir de un canal de propagación (EUC_CP), estando dichas claves destinadas a proteger datos intercambiados entre un primer usuario y un segundo usuario, constando un usuario de uno o varios emisores y uno o varios receptores, siendo los datos transmitidos por el canal de propagación, caracterizado porque cada usuario consta al menos de una unidad de cálculo adaptada a ejecutar las etapas del procedimiento según la invención.

Los emisores y los receptores son, por ejemplo, emisores/receptores de radiocomunicaciones, o emisores y receptores adaptados a las transmisiones acústicas o incluso emisores y receptores de transmisiones ópticas.

Otras características y ventajas de la presente invención serán más evidentes con la lectura de la descripción que se da a título ilustrativo y en absoluto limitativo, junto con las figuras que representan:

- La figura 1, un esquema general de intercambios de información entre dos usuarios A (Alice) y B (Bob) en presencia de un tercero extraño E (Eve) no autorizado a conocer el contenido de los datos intercambiados entre A y B,
- La figura 2, una ilustración de los efectos de un canal de propagación dispersivo sobre la transmisión de las señales desde un emisor (A) hacia un receptor autorizado (B) y hacia un receptor no autorizado (E), y
- La figura 3, un esquema que explica un algoritmo de cuantificación del canal de propagación entre el emisor A y el receptor B, después de la medida de este por B según procedimientos bien conocidos por el experto en la materia.

Para hacer entender mejor el procedimiento según la invención, se da el ejemplo en el caso de un intercambio entre un primer usuario emisor/receptor A (Alice) y un segundo usuario emisor/receptor B (Bob), en presencia de un receptor tercero E (Eve) no autorizado, susceptible de interceptar las comunicaciones y de acceder al contenido de los datos intercambiados entre A y B.

La figura 1 ilustra un escenario de comunicación entre un primer usuario A, 10 y un segundo usuario B, 20 en presencia de un receptor tercero no autorizado E, 30.

El usuario A es, por ejemplo, un nodo o un terminal de una red de comunicación que consta de una unidad de

cálculo 11, un módulo de codificación/decodificación 12, un módulo de desmodulación 13, un módulo compuesto por antenas 14, un conjunto de filtros 15, medios de emisión y recepción por radio 16e, 16r. Estos elementos son conocidos por el experto en la materia y no se detallarán. El objeto de la invención consistirá, en concreto, en la ejecución de un algoritmo que permita el cálculo de una clave aprovechando las medidas efectuadas en los parámetros del canal como se explicará más adelante.

Del mismo modo, el usuario B, 20, consta, por ejemplo, de una unidad de cálculo 21, un módulo de codificación/decodificación 22, un módulo de desmodulación 23, un módulo compuesto por antenas 24, filtros 25, medios de emisión y recepción por radio 26e, 26r.

El receptor tercero no autorizado E, 30, consta de una unidad de cálculo 31, un grabador de datos 32 y un módulo de análisis 33, un bloque de antenas 34 y filtros 35 y medios de recepción por radio 36.

La figura 2 esquematiza un ejemplo de canales de propagación existentes en un sistema de comunicación. En entornos exteriores o interiores, las formas de onda transmitidas del emisor A hacia el receptor B (flecha I, figura 1) y hacia el tercero E (flecha II, figura 1) siguen recorridos multitrayecto. Las señales pueden ser reflejadas por obstáculos con diferentes ángulos de reflexión. Una parte de las señales S_{AB} puede ser recibida por Bob, mientras que otra parte después de la difracción S_{AE}, será recibida por el tercero no autorizado E. Debido a la complejidad en la propagación de las ondas y a las difracciones poco previsibles en el canal de comunicación, el tercero E es, a priori, incapaz de predecir o de reconstituir las medidas del canal de propagación entre el emisor A y el receptor B para comunicar. Es, en concreto, esta característica la que utilizará el procedimiento según la invención. Los canales medidos por Alice y por Bob y los coeficientes que extraerán de ellos, después de la cuantificación y un formateo apropiados descritos más adelante, caracterizan los enlaces "legítimos", autorizados y no podrán ser ni conocidos ni reconstruidos por el tercero E.

Al desear los emisores/receptores Alice A y Bob B comunicar con total seguridad, A y B quieren extraer una clave secreta común K_A, a partir de los parámetros del canal de propagación que mide cada uno. Por ejemplo, cuando el tercero no autorizado Eve E está situado a una distancia de varias longitudes de onda de B, las medidas de canal siempre serán independientes del canal legítimo y, de hecho, la clave K_E que E podrá extraer será independiente de la clave secreta K_A extraída por A y B. En numerosos casos, una distancia de varias longitudes de ondas basta para garantizar la independencia entre las claves K_A y K_E.

Considerando intercambios entre usuarios A y B en modo dúplex temporal (emisión y recepción en la misma frecuencia portadora en el sentido A hacia B y B hacia A), la invención aprovecha la reciprocidad natural del canal de propagación (durante su periodo de estacionariedad) en la medida en que los ángulos de incidencia y las longitudes de los trayectos de ida y vuelta son iguales.

Considerando intercambios entre usuarios A y B en modo dúplex frecuencial (emisión y recepción en frecuencias portadoras diferentes según el sentido A hacia B o B hacia A), la implementación de la invención pasa por la duplicación en cada portadora, de las etapas del procedimiento descritas en lo sucesivo para aprovechar la reciprocidad natural del canal de propagación en cada una de las portadoras.

Siendo el objetivo generar una clave secreta para proteger los intercambios de datos entre el emisor/receptor A y el emisor/receptor B, el procedimiento implementará, por ejemplo, las etapas siguientes:

a) La primera etapa consiste en medir las señales emitidas por cada emisor 16e de un primer usuario A después de la recepción de las señales en cada receptor 26r del segundo usuario B, en estimar los parámetros de los canales de propagación correspondientes, y a continuación en calcular las respuestas complejas (con información de amplitud y de fase) en frecuencia o en tiempo de los canales correspondientes. Estas estimaciones son realizadas por los receptores 26r de B en los emisores 16e de A y por los receptores de A 16r en los emisores 26e de B. Permiten obtener los valores de los parámetros de los canales de propagación, por ejemplo, las respuestas impulsionales complejas y/o respuestas en frecuencia complejas de dichos canales de propagación;
b) Durante una segunda etapa, el procedimiento utiliza un algoritmo ejecutado en la unidad de cálculo 11, 12, de cada uno de los usuarios A y B que permite seleccionar de forma univalente los coeficientes complejos de canales de propagación resultantes de las estimaciones realizadas en la etapa a), conservando solamente los coeficientes que presentan una pequeña correlación cruzada, inferior a un umbral predeterminado ajustable V_{CC}. La clave secreta Ks extraída al final del proceso lo será entonces con un carácter aleatorio suficiente, incluso en entornos de propagación muy estacionarios encontrados, por ejemplo, cuando los emisores y receptores son de posiciones fijas y que los obstáculos y reflectores que intervienen en los mecanismos de propagación son, ellos también, fijos;
c) Durante una tercera etapa, llamada cuantificación y formateo, cada usuario realiza una cuantificación de los coeficientes complejos de canales seleccionados, aplicando una malla geométrica del plano complejo, una numeración de los coeficientes complejos del canal según la malla a la que pertenecen y un formateo unívoco de los datos cuantificados, para aumentar su fiabilidad mediante técnicas de corrección de errores aplicadas a dicha numeración, por ejemplo el empleo de dos planos de cuantificación alternos, tal como lo presenta Wallace. Esto permite minimizar, a priori, las diferencias entre las claves obtenidas por los usuarios legítimos - clave K_A

obtenida por A en las emisiones de B y clave K_B obtenida por B en las emisiones de A;
d) Durante una cuarta etapa, opcional, llamada etapa de reconciliación de la información, el procedimiento elimina la discrepancia que queda entre la clave K_A obtenida por A y la clave K_B obtenida por B. Para ello, se utilizan, por ejemplo, códigos correctores de errores e intercambios con poca revelación de información según la descripción a continuación, para corregir los errores de B en la clave K_A de A, en el caso en que K_B fuera diferente de K_A al final de las etapas precedentes. Alice A transmitirá por ejemplo en el canal público un mensaje que no revelará el valor de la clave K_A, pero que permitirá a Bob B recuperar la clave K_A a partir de la clave K_B que el mismo ha determinado, considerada como una aproximación imperfecta de K_A. Debido a la fuerte descorrelación del canal de propagación entre A y E y entre B y E, la clave extraída del canal de propagación por E en las emisiones de A o de B, K_E, será demasiado diferente de las claves K_A o K_B calculadas por A y B para permitir a E recuperar K_A o K_B;
e) Una quinta etapa opcional, llamada amplificación de la confidencialidad, se implementa utilizando, por ejemplo, una función de troceado. Esta etapa permitirá eliminar cualquier revelación residual de información hacia un tercero E no autorizado, y mejorar al mismo tiempo el carácter aleatorio de la clave secreta K_A. Esta etapa permite garantizar que la clave secreta K_S generada a la salida es independiente de cualquier clave K_E eventualmente calculada por el tercero no autorizado, incluso si E puede captar, decodificar e interpretar adecuadamente todas las informaciones intercambiadas entre A y B.

El código corrector de errores en la etapa d) de reconciliación puede ser un simple código algebraico, bien conocido por el experto en la materia y la función de troceado utilizada en la etapa e) de amplificación de la confidencialidad, una familia 2-universal de funciones de troceado, conocida por el experto en la materia.

Las etapas opcionales d) y e) se pueden optimizar cuando los usuarios tienen garantías suficientes sobre la fiabilidad y el secreto de las etapas a) b) y c), en este caso tenemos directamente $K_S=K_A=K_B$.

Las etapas del procedimiento resumidas anteriormente se detallarán a continuación.

Estimación del canal de propagación (etapa a)

La generación de clave secreta K_S se basa en la utilización de la información sobre el estado del canal de propagación, conocida con la expresión anglosajona "Channel State Information". Esta información se puede medir en el dominio frecuencial (Channel Frequency Response (CFR) en inglés o Channel Transfert Function (CTF)) indicada como H_f en lo sucesivo, o en el dominio temporal (Channel Impulse Response en inglés o CIR), indicada como H_t en lo sucesivo.

En el dominio frecuencial, la estimación del canal H_f cuantifica el desvanecimiento o fading aplicado en cada subportadora.

En un sistema en el que las señales son adecuadamente (es decir, según las reglas conocidas por el experto en la materia - respecto al criterio de Nyquist) filtradas y muestreadas en banda de base con un periodo T_{ech}, considerando una respuesta de canal de ancho de banda finito, la $k^{ésima}$ componente de la respuesta CFR muestreada $\hat{H}_f(k)$ correspondiente a la frecuencia $f_k = k/T_{ech}$ se calcula según la fórmula:

$$\hat{H}_f(k) = \frac{Y(f_k)}{X(f_k)}$$

donde $Y(f_k)$ es la señal recibida en el dominio frecuencial a la frecuencia f_k, $X(f_k)$ es la señal emitida o la señal de referencia en el dominio frecuencial a la frecuencia f_k.

Este procedimiento está particularmente bien adaptado para formas de ondas multiportadoras que utilizan una modulación de codificación por distribución en frecuencia ortogonal o OFDM (Orthogonal Frequency Division Multiplexing), por ejemplo WiFi, LTE, Bluetooth.

La respuesta CFR muestreada $\hat{H}_f(k)$ también se puede obtener mediante el aprovechamiento directo de las salidas de los procesamientos aplicados en el dominio frecuencial por los receptores de cada usuario para las necesidades propias de la calidad de su recepción y desmodulación de las señales emitidas por los otros usuarios: igualación en subportadoras piloto en los nodos, estaciones de base y terminales que emplean técnicas de acceso por radio a las modulaciones de tipo OFDM y protocolos asociados, por ejemplo de tipo O-FDMA (Orthogonal-Frequency Division Multiple Access) o SC-FDMA (Single Carrier-Frequency Division Multiple Access) como en las redes de radiodifusión con la norma DVB-T (Digital Video Broadcast-Terrestrial), o las redes radiocelulares de cuarta generación con la norma LTE (Long Term Evolution), siendo estas técnicas bien conocidas por el experto en la materia.

En el dominio temporal, la estimación del canal H_t cuantifica la distribución de los trayectos de propagación a lo largo del tiempo en la banda de la portadora de la señal. En el ejemplo dado, considerando una aproximación finita de la respuesta temporal del canal, la $l^{ésima}$ muestra de la respuesta CIR muestreada $H_t(l)$, correspondiente al instante $t_l=l.T_{ech}$, la respuesta CIR $H_t(l)$ muestreada se obtiene, por ejemplo, a partir de la respuesta CFR muestreada utilizando la transformación de Fourier rápida inversa como sigue:

$$H_t = IFFT(\hat{H}_f).$$

También se puede obtener directamente en el dominio temporal a partir de señales de referencia $x_A(t+t_0)$ y $x_B(t+t_0)$ emitidas por los usuarios A y B, a partir de un instante de referencia t_0, y aplicando, a las señales $y_A(t+t_0)$ e $y_B(t+t_0)$ recibidas por los receptores de los usuarios A y B después de la propagación en el canal de transmisión del que se considera una aproximación de longitud finita L, las etapas siguientes:

- un filtrado y un muestreo adecuados (respecto al criterio de Nyquist conocido por el experto en la materia) en banda de base con el periodo T_{ech} que produce las señales muestreadas $y_A(I+I_0)$ e $y_B(I+I_0)$, estando los índices I e I_0 definidos por $t=I.T_{ech}$; $t_0=I_0.T_{ech}$,
- utilizar uno o varios procedimientos de estimación de filtros con respuesta finita (procedimientos conocidos por el experto en la materia), para, por ejemplo, estimar los coeficientes $H_t(l_1)$, $l_1 = 0,..., L - 1$ minimizando una función no lineal que traduce, en un periodo de integración de L muestras, el error cuadrático de estimación entre la señal muestreada recibida $y(I+I_0)$ y la señal muestreada emitida $x(I+I_0)$ filtrada por el canal de propagación muestreado $H_t=\{H_t(l_1)_{l1=0,...,L-1}\}$.

Dicha función se explica en la fórmula siguiente:

$$\left\{H_t(l_1)_{l_1=0\ ,...,L-1}\right\} = ArgMin_{\{h(l_1)_{l_1=0\ ,...,L-1}\}}\left\{\sum_{l=0}^{L'-1}\left\|y(l_0+l)-\sum_{l_1=0}^{L-1}h(l_1)\,x(l_0+l-l_1)\right\|^2\right\}$$

La respuesta CIR $H_t(I)$ muestreada también se puede obtener por el aprovechamiento directo de las salidas de los procesamientos aplicados en el dominio temporal por los receptores de cada usuario, para las necesidades propias de la calidad de su recepción y desmodulación de las señales emitidas por los otros usuarios:

- igualación en secuencias piloto en los nodos, estaciones de base y terminales que emplean técnicas de acceso por radio a los protocolos TDMA (Time Division Multiple Access) como en las redes de segunda generación con la norma GSM (Global System Mobile),
- recepción por radio RAKE en los nodos, estaciones de base y terminales que emplean técnicas de acceso por radio a los protocolos CDMA (Code Division Multiple Access) como en las redes de tercera generación con la norma UMTS (Universal Mobile Terrestrial System),

siendo estas técnicas conocidas por el experto en la materia.

Descorrelación de canal (etapa b)

Las claves secretas K_s generadas deben ser, preferentemente, totalmente aleatorias para ser impredecibles por el tercero no autorizado E. Para ello, la segunda etapa del procedimiento (etapa b) utiliza un algoritmo de selección en los dominios temporal y frecuencial que permiten conservar solamente los coeficientes de canales descorrelacionados, es decir que presentan la capacidad de generar datos digitales o bits con distribuciones de probabilidades iguales y no correlacionadas.

Para eliminar la correlación temporal y frecuencial, el procedimiento puede, por ejemplo, implementar uno u otro de los algoritmos descritos a continuación.

Se puede utilizar un algoritmo de disminución de la correlación temporal entre los coeficientes de canales. El conjunto de los coeficientes de canales medidos en un mismo instante de adquisición t constituye una trama temporal. Los coeficientes temporales de correlación cruzada $C_{cc,t}$ se calculan entre dos tramas consecutivas R_i, R_{i+1} mediante algoritmos conocidos por el experto en la materia. El procedimiento selecciona las tramas para las cuales el coeficiente de correlación cruzada $C_{cc,t}$ es inferior a un valor umbral $\boldsymbol{T_t}$.

También es posible utilizar un algoritmo de disminución de la correlación frecuencial entre los coeficientes del canal. El procedimiento se explica a continuación, a título ilustrativo y no limitativo, para una señal de modulación por subportadora de tipo OFDM (Orthogonal Frequency Division Multiplexing). Para dicha señal, los coeficientes frecuenciales de correlación cruzada $C_{cc,f}$ se calculan entre dos frecuencias portadoras consecutivas P_j, P_{j+1} mediante algoritmos conocidos por el experto en la materia. El procedimiento selecciona las portadoras para las cuales el coeficiente de correlación cruzada $C_{cc,f}$ es inferior a un valor umbral $\boldsymbol{T_f}$. Además, las subportadoras de frecuencia más baja y de frecuencia más alta se eliminan. El procedimiento se aplicaría de la misma manera a las componentes espectrales complejas de una señal general, en las salidas de una transformación de Fourier de dicha señal llevada a cabo según las reglas de la técnica.

Finalmente, Alice transmitirá a Bob los índices temporales t y frecuenciales f de los coeficientes de canales

seleccionados, pasando por el canal público de transmisión. Solo se transmiten los índices de estos coeficientes, lo que no induce ninguna divulgación de información sobre el valor de estos coeficientes hacia un tercero no autorizado E.

Un segundo algoritmo de descorrelación de las medidas del canal procede por concatenación de los dos algoritmos anteriores, como sigue: primeramente se preseleccionan las tramas temporales $C_{cc,t}$ para las cuales los coeficientes de correlación cruzada con todas las demás tramas son todos inferiores a un umbral fijado T_t. A continuación, para las tramas temporales resultantes de la preselección anterior, se seleccionan las frecuencias portadoras para las cuales los coeficientes de correlación cruzada $C_{cc,f}$ son todos inferiores a un umbral fijado T_f.

Cuantificación (etapa c)

Tomando como hipótesis que el canal de propagación es recíproco y aleatorio, se puede considerar como una fuente común de bits aleatorios b_i entre un par de terminales legítimos donde i es un índice entero. De este modo, después de medir el canal de radio, el emisor 16e de A y el receptor 26r de B utiliza conjuntamente un algoritmo de cuantificación para generar una secuencia de bits $b_1,...b_N$, destinados a producir una clave secreta a partir del canal común a A y B. Sin embargo, debido a la presencia de ruido y de errores de estimación del canal de propagación, el emisor 16e de A y el receptor 26r de B pueden estar en discrepancia en algunos bits de la clave secreta generada, es decir que las claves K_A y K_B no coinciden en su totalidad. Para limitar este fenómeno, el procedimiento ejecutará un algoritmo de cuantificación adaptado.

Un ejemplo convencional de algoritmo de cuantificación consiste en tejer el plano complejo (llamado entonces plano de cuantificación) en el que los coeficientes de canales asumen sus valores. Convencionalmente, el eje real y el eje imaginario del plano complejo se dividen en intervalos, con bandas de guarda entre estos intervalos. El algoritmo de cuantificación atribuye a un coeficiente complejo de canal los números de los intervalos en los que se encuentran su parte real y su parte imaginaria, pero rechaza todas las partes reales o imaginarias de coeficientes complejos que se sitúan en el exterior de un intervalo, es decir en una de las bandas de guarda, lo que conduce de este modo a un aprovechamiento ineficaz de las medidas de canal y a un número reducido de datos digitales o bits extraídos.

Otros esquemas utilizan planos de cuantificación múltiples, donde cada plano está adaptado a la trama actual de los coeficientes de canales, tal como el algoritmo de cuantificación de canal CQA descrito en el documento de J. Wallace y R. Sharma, "Automatic secret keys from reciprocal MIMO Wireless channels: measurement and analysis", IEEE Trans. on Info. Foren. and Sec., vol. 5, no. 3, págs. 381-392, septiembre de 2010. El principio implementado consiste en elegir el plano de cuantificación menos sensible a la discrepancia de la trama actual de los coeficientes de canales.

El procedimiento según la invención aplicará, por ejemplo, un algoritmo CQA a los coeficientes de canales para generar los bits de la clave secreta.

Un ejemplo ilustrativo y no limitativo se da en la figura 3 que ilustra el principio del algoritmo CQA. Este algoritmo utiliza dos planos alternos para generar los bits de la clave secreta. La figura 3 ilustra la aplicación del algoritmo CQA considerando solamente un solo eje para simplificar, por ejemplo el eje real y las partes reales de los coeficientes complejos de canales.

La función de distribución de las partes reales e imaginarias de los coeficientes complejos de canal se utiliza para dividir el espacio de medidas en regiones equiprobables. El conjunto de estas regiones constituyen entonces un primer plano de cuantificación P0. Un segundo plano de cuantificación P1 se obtiene después de la traslación del primero, según un esquema descrito en el documento de J. Wallace y R. Sharma, mencionado anteriormente. De este modo, para cada observación, el emisor de A elige el plano de cuantificación para el cual la medida es la más alejada de una frontera, para minimizar el riesgo de error después de la cuantificación. A continuación, el emisor de A transmite al receptor de B un mensaje M_A en el canal público que indica cuál es el plano de cuantificación utilizado para cada medida de canal. Este mensaje solamente revela el índice del plano de cuantificación utilizado y ninguna información sobre el valor de los coeficientes del canal.

En el ejemplo dado en la figura 3, el espacio total de las medidas de canal observables se divide en ocho regiones QM numeradas M=0 a M=7. Cuando esta división en ocho regiones se aplica directamente, los errores de ruido y de estimación pueden generar "discrepancias" frecuentes entre las medidas de canal del emisor de A y del receptor de B en las inmediaciones de las fronteras entre regiones.

En la figura ilustrativa 3, dos planos alternos P0 y P1 de cuatro regiones se deducen del mapa original en 8 regiones QM, M= 1,...,7. Para cada coeficiente de canal, Alice elige el plano de cuantificación P0 o P1 para el cual el coeficiente de canal es el más lejano de una frontera, reduciendo de este modo la probabilidad de discrepancia.

Por ejemplo en la figura 3, Alice elige el plano P1 para cuantificar el coeficiente de canal y obtener como bit de clave cero. Alice transmite a continuación a Bob el índice 1 del plano P1 seleccionado. A partir de este identificador, Bob genera también el cero como bit de clave utilizando la medida de canal. Al final, en este ejemplo, a pesar de un error posible entre las medidas de canal de A y de B debido a los ruidos de recepción y medida, A y B generarán la misma clave secreta.

Etapa de reconciliación (etapa d)

Durante la etapa de reconciliación, el procedimiento suprimirá las discrepancias restantes entre la clave generada por A, K_A, y la clave generada por B, K_B, utilizando un código corrector de errores. La clave calculada por A, K_A, se considera como la clave secreta y B quiere recuperar la clave de A, K_A, corrigiendo la clave K_B extraída de sus propias medidas de canal.

La etapa de reconciliación comprende, por ejemplo, las etapas siguientes:

A nivel de A:

- Selección de una palabra aleatoria ***c*** que pertenece a un código corrector de errores $\mathcal{C}$,
- Cálculo del mensaje $\boldsymbol{s} = \boldsymbol{K_A} \oplus \boldsymbol{c}$ llamado secure sketch, término conocido por el experto en la materia, $\oplus$ designa el módulo de adición 2,
- Transmisión del secure sketch ***s*** a Bob utilizando el canal de comunicación público,

A nivel de B:

- Utilización del secure sketch ***s*** para calcular la palabra $\boldsymbol{c_B}$ que pertenece al código corrector $\mathcal{C}$ y que corresponde a la clave de B, $\boldsymbol{K_B}$: $\boldsymbol{c_B} = \boldsymbol{K_B} \oplus \boldsymbol{s}$, $\boldsymbol{c_B}$ representa de este modo una aproximación imperfecta de la palabra aleatoria ***c*** seleccionada por A,
- Decodificación de $\boldsymbol{c_B}$ para corregir los errores y recuperar la palabra de código ***c*** seleccionado por A. B obtiene entonces $\hat{\boldsymbol{c}}$, una estimación de ***c***,
- Recuperación de K_A a partir de la palabra de código decodificada $\hat{\boldsymbol{c}}$ y del secure sketch ***s***: $\boldsymbol{K_A} = \hat{\boldsymbol{c}} \oplus \boldsymbol{s}$.

La etapa de reconciliación tiene éxito cuando B consigue decodificar perfectamente la palabra de código ***c*** seleccionada por Alice, es decir cuando $\hat{\boldsymbol{c}} = \boldsymbol{c}$. De este modo, B recupera el valor exacto de la clave de A: $\boldsymbol{K_A} = \boldsymbol{K_A}$.

Por consiguiente, aunque transmitido en el canal público, el secure sketch permite la recuperación exacta de la clave secreta $\boldsymbol{K_A}$ sin revelar su valor exacto.

No obstante, E también puede utilizar el secure sketch para acercarse a la clave secreta $\boldsymbol{K_A}$. Es necesario, entonces, suprimir la información que se hizo vulnerable por el envío del secure sketch en el canal público.

Una última etapa permite suprimir esta fuga de información y mejorar la calidad de la clave secreta.

Etapa de amplificación de la confidencialidad (etapa e)

Como ya se mencionó anteriormente, el objetivo de esta última etapa es suprimir la información que pudo huir hacia el tercero E durante la etapa de reconciliación y mejorar el carácter aleatorio de la clave. Para obtener este resultado, es posible utilizar funciones de troceado.

El siguiente ejemplo se da para una familia "2-universal" de funciones de troceado.

Una familia $\mathcal{G}$ de funciones $\mathcal{A} \rightarrow \mathcal{B}$ se denomina 2-universal si para x1 ≠ x2:

$$\Pr[g(x_1) = g(x_2)] \leq \frac{1}{|\mathcal{B}|}$$

donde g se selecciona de manera aleatoria en $\mathcal{G}$

Una manera de construir una familia 2-universal es seleccionar un elemento aleatorio $\boldsymbol{a} \in \boldsymbol{GF}(\boldsymbol{2^n})$ e interpretar la clave secreta $\boldsymbol{K_A}$ como un elemento de $\boldsymbol{GF}(\boldsymbol{2^n})$.

La función $\{\boldsymbol{0,1}\}^{\boldsymbol{n}} \rightarrow \{\boldsymbol{0,1}\}^{\boldsymbol{r}}$ que asigna a $\boldsymbol{K_A}$ los ***r*** primeros bits del producto $\boldsymbol{a}.\ \boldsymbol{K_A} \in \boldsymbol{GF}(\boldsymbol{2^n})$ es una familia 2-universal de funciones de troceado para $\boldsymbol{1} \leq \boldsymbol{r} \leq \boldsymbol{n}$.

Cabe destacar que $\boldsymbol{a}.\ \boldsymbol{K_A}$ es un producto definido en el cuerpo de Galois $\boldsymbol{GF}(\boldsymbol{2^n})$.

Las etapas del procedimiento detalladas anteriormente se pueden repetir de una transmisión de datos a otra transmisión y/o regularmente dentro de una misma transmisión. El procedimiento recalcula el código secreto con cada nueva transmisión y con cada nuevo mensaje en función del control de potencia y de las fluctuaciones de propagación y de las adaptaciones de velocidad de transferencia eventuales.

El procedimiento se puede implementar dentro de un sistema de transmisión que utiliza un protocolo de ruido y de

formación de haz para la transmisión de los datos, siendo entonces las señales, señales emitidas y recibidas en el marco de dicho protocolo de ruido artificial y formación de haz.

Las señales también pueden ser señales emitidas y recibidas en el marco de un protocolo con emisión y recepción simultáneas.

Según otra variante de realización, las señales utilizadas para la extracción de claves son señales de marcado, públicas o no, encubiertas o no, con o sin autointerferencia, emitidas y recibidas en el marco de un protocolo de identificación de sistemas de emisión-recepción o en el marco de un protocolo de autentificación de usuarios de dicho sistema o en el marco de un protocolo de control de integridad de los mensajes emitidos y recibidos por dicho sistema.

Los emisores y los receptores del dispositivo se seleccionarán, por ejemplo, entre la lista siguiente: emisores y receptores adaptados a radiocomunicaciones, emisores y receptores adaptados a transmisiones acústicas, emisores y receptores adaptados a transmisiones ópticas.

Ventajosamente el procedimiento según la invención permite extraer una clave secreta de manera univalente y unívoca, permitiendo de este modo la protección de los datos intercambiados entre usuarios.

REIVINDICACIONES

1. Procedimiento de extracción univalente y unívoca de claves a partir de un canal de propagación (EUC_CP), estando dichas claves destinadas a proteger datos intercambiados entre un primer usuario A y un segundo usuario B, constando un usuario de uno o varios emisores (16e, 26e) y uno o varios receptores (26e, 26r), siendo los datos transmitidos por el canal de propagación, que consta al menos de las etapas siguientes:

a) Medir mediante el o los receptores (16r, 26r) del primer y del segundo usuario A, B, señales S que provienen de cada emisor (16e, 26e) del otro usuario, medir los parámetros del canal de propagación correspondiente y, a continuación, estimar las respuestas impulsionales complejas correspondientes de canal de propagación o respuestas en frecuencias complejas correspondientes del canal de propagación,
b) Seleccionar de manera univalente, para cada usuario A, B, un conjunto de coeficientes complejos de canal resultantes de las estimaciones de las respuestas impulsionales complejas del canal de propagación o de las respuestas en frecuencia complejas del canal de propagación, y conservar los coeficientes que presentan una correlación cruzada inferior a un valor umbral predeterminado ajustable,
c) Cuantificar y formatear, para cada usuario, los coeficientes complejos de canal seleccionados, aplicando una malla geométrica del plano complejo en el que los coeficientes de canal asumen su valor, una numeración de los coeficientes complejos según la malla a la que pertenecen, y técnicas de corrección de errores en dicha numeración,
d) Utilizar de manera univalente y unívoca, para cada usuario, datos digitales resultantes de dicha cuantificación y de dicho formateo en forma de claves secretas para encriptar la cadena de datos transmitidos.

2. Procedimiento según la reivindicación 1, **caracterizado porque** utiliza un modo de comunicación entre usuarios, un modo dúplex temporal que emplea una misma frecuencia portadora para los intercambios en emisión y en recepción en los dos sentidos de transmisión.

3. Procedimiento según la reivindicación 1, **caracterizado porque** está duplicado en el conjunto de las frecuencias portadoras empleadas por usuarios en modo dúplex frecuencial que emplea frecuencias portadoras diferentes para sus intercambios en emisión y en recepción según el sentido de transmisión.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque** aplica una función de codificación correctora de errores en las claves extraídas K_A, K_B por los usuarios A, B, con una transmisión mínima de datos del primer usuario hacia el segundo, para eliminar las diferencias entre las claves del primer y del segundo usuario.

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado porque** utiliza una función de troceado y una reducción de longitud en las claves extraídas adaptadas para eliminar cualquier fuga residual de información hacia un tercero mejorar las calidades aleatorias de las claves.

6. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** se repiten las etapas de una transmisión de datos a otra y regularmente dentro de una misma transmisión.

7. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** se utiliza un protocolo de ruido y de formación de haz para la transmisión de los datos y **porque** las señales son señales emitidas y recibidas en el marco de dicho protocolo de ruido artificial y formación de haz.

8. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** las señales son señales emitidas y recibidas en el marco de un protocolo con emisión y recepción simultáneas.

9. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** las señales son señales de marcado, públicas o no, encubiertas o no, con o sin autointerferencia, emitidas y recibidas en el marco de un protocolo de identificación de sistemas de emisión-recepción o en el marco de un protocolo de autentificación de usuarios de dicho sistema o en el marco de un protocolo de control de integridad de los mensajes emitidos y recibidos por dicho sistema.

10. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** utiliza emisores y receptores adaptados a radiocomunicaciones.

11. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** los emisores y receptores están adaptados a transmisiones acústicas.

12. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** los emisores y receptores están adaptados a transmisiones ópticas.

13. Dispositivo que permite una extracción univalente y unívoca de claves a partir de un canal de propagación (EUC_CP) y que comprende una unidad de cálculo, estando dichas claves destinadas a proteger datos intercambiados entre un primer usuario y un segundo usuario, constando un usuario A, B de uno o varios emisores (16e, 26e) y uno o varios receptores (16r, 26r), siendo los datos transmitidos por el canal de propagación, en el que cada usuario consta al menos de una dicha unidad de cálculo adaptada a ejecutar las etapas del procedimiento

según una de las reivindicaciones 1 a 12.

14. Dispositivo según la reivindicación 13, **caracterizado porque** los emisores y los receptores son emisores/receptores de radiocomunicaciones.

15. Dispositivo según la reivindicación 13, **caracterizado porque** los emisores y los receptores son emisores/receptores de transmisiones acústicas.

16. Dispositivo según la reivindicación 13, **caracterizado porque** los emisores y los receptores son emisores y receptores de transmisiones ópticas.

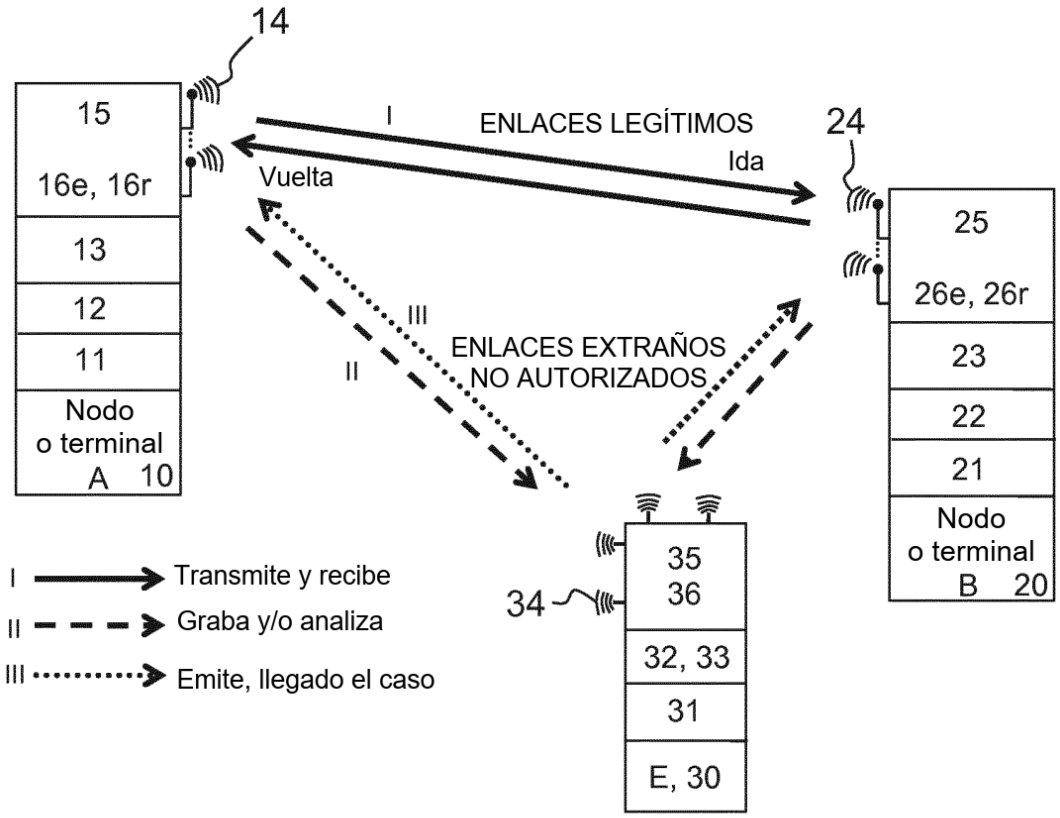
14
15
16e, 16r
13
12
11
Nodo
o terminal
A 10
I
ENLACES LEGÍTIMOS
Ida
Vuelta
24
25
26e, 26r
23
22
21
Nodo
o terminal
B 20
III
II
ENLACES EXTRAÑOS
NO AUTORIZADOS
34
35
36
32, 33
31
E, 30
I Transmite y recibe
II Graba y/o analiza
III Emite, llegado el caso

FIG.1

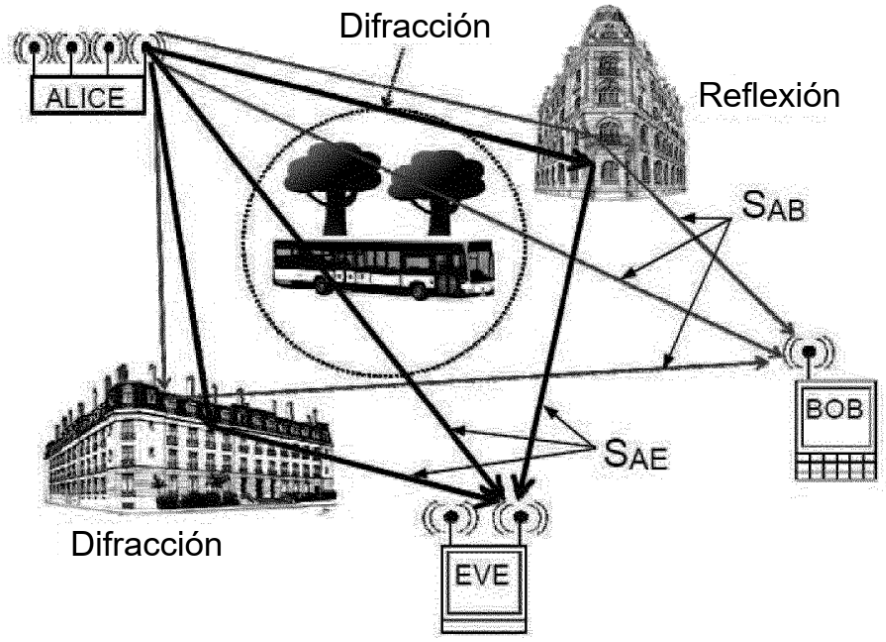
Difracción
ALICE
Reflexión
SAB
BOB
SAE
Difracción
EVE

FIG.2

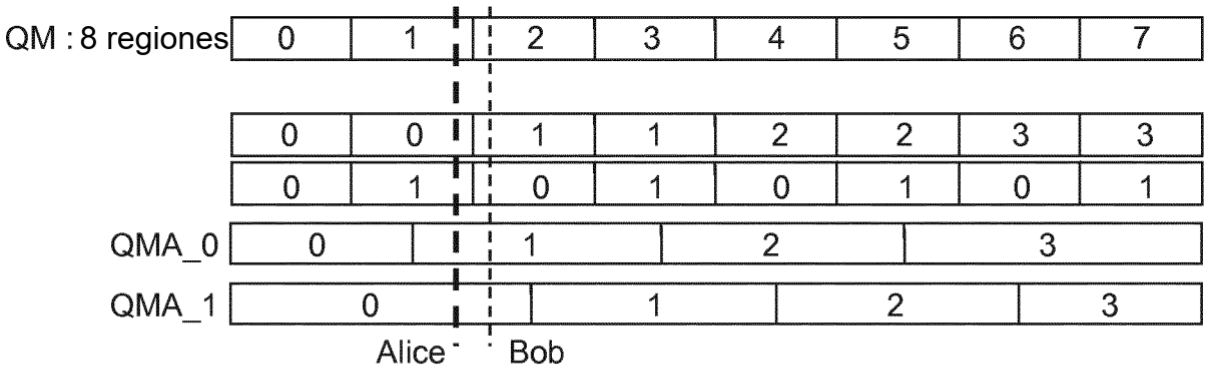
QM : 8 regiones
0
1
2
3
4
5
6
7
0
0
1
1
2
2
3
3
0
1
0
1
0
1
0
1
QMA_0
0
1
2
3
QMA_1
0
1
2
3
Alice
Bob

FIG.3