(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 428 381**

(51) Int. CI.:

H04L 9/30 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.05.2008 E 08757518 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.07.2013 EP 2124381**

(54) Título: **Método, sistema y dispositivo para generar una clave de grupo**

(30) Prioridad:

08.06.2007 CN 200710100375

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.11.2013

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian
Longgang District, Shenzhen
Guangdong 518129 , CN

(72) Inventor/es:

XU, CHUNXIANG;
ZHONG, HUAN y
LIU, YA

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, sistema y dispositivo para generar una clave de grupo

Campo de la invención

La presente invención está relacionada con el campo de las comunicaciones de red y, más en particular, con un método, un sistema y un dispositivo para generar una clave de grupo.

Antecedentes de la invención

Una red Ad Hoc es una red independiente de múltiples saltos con una estructura topológica que cambia de forma dinámica, en la cual frecuentemente los nodos se mueven y están limitados en potencia, y son más bien pobres la relación de confianza y los enlaces de transmisión inalámbricos entre los nodos. Así, el diseño de un protocolo de negociación de una clave de grupo en la red Ad Hoc es considerablemente diferente respecto a una solución convencional. En la red Ad Hoc, para garantizar la seguridad de las comunicaciones, en general los mensajes se cifran y después se transmiten. Debido a la ventaja en eficiencia de un sistema de cifrado simétrico, se reduce enormemente la complejidad del procesamiento de mensajes mediante la compartición de una clave dentro del grupo. En otro orden de cosas, la red Ad hoc también es un grupo dinámico de pares, y carece del soporte de una tercera parte fija confiable de modo que es necesario establecer, mediante la negociación de todos los miembros del grupo, una clave de sesión del grupo para cifrar los mensajes, con el fin de mejorar la seguridad y fiabilidad de la clave de sesión del grupo. Además, en la red Ad Hoc es necesario que el protocolo de negociación de la clave del grupo tenga en cuenta las características de topología dinámica de la red, y garantice seguridad posterior y seguridad anterior de la clave y soporte de forma eficiente los movimientos de incorporación y salida de los nodos.

Todas las soluciones existentes de negociación de la clave de grupo se basan en el problema de logaritmo discreto en el campo finito. Existe una solución de negociación de la clave de grupo aplicable a la red Ad Hoc en la que n representa el número de miembros del grupo; U_i representa un miembro del grupo con un número de serie i; U_1 representa un organizador seleccionado, y el organizador es temporal y puede ser ejercido por cualquier miembro. La FIG. 1 es un diagrama de flujo de un método de una solución de negociación de la clave de grupo en la técnica anterior. Haciendo referencia a la FIG. 1, la solución de negociación de la clave de grupo incluye:

101: Se seleccionan parámetros del sistema y se lleva a cabo una inicialización del sistema.

Suponiendo que p y q son número primos grandes, Z_p es un conjunto formado por el módulo entero de p, g es un elemento en Z_p, y q es un orden de g, en el que q es el mínimo entero positivo que satisface una ecuación $g^q \equiv 1 \bmod q$.

102: Todos los miembros seleccionan valores DH secretos, generan valores DH públicos en función de los valores DH secretos y difunden en el grupo los valores DH públicos generados. El miembro U_i del grupo selecciona de forma aleatoria un valor DH secreto $r_i \in Z_q$, genera un valor DH público g^{r_i} en función del valor DH secreto seleccionado y difunde en el grupo el valor DH público g^{r_i} generado, en el que i tiene el valor de 1,2, …, n.

103: Después de recibir los valores DH públicos del resto de miembros, un organizador selecciona un exponente secreto, genera un mensaje intermedio en función del exponente secreto y los valores DH públicos y difunde en el grupo el mensaje intermedio, y al mismo tiempo genera una clave de grupo.

El organizador U_1 selecciona de forma aleatoria un exponente secreto $v \in Z_q$, genera un mensaje intermedio M_i, $M_i = v \cdot g^{r_1 r_i}$ en función del exponente secreto, un valor DH público del propio organizador, y los valores DH públicos del resto de miembros, respectivamente, y difunde en el grupo el mensaje M_i generado, en el que i tiene el valor de 1, 2, …, n.

Específicamente, el organizador calcula una función $F = f(g^{r_2}, g^{r_3}, \cdots, g^{r_n})$ en función del valor DH público de cada miembro y el valor DH público del propio organizador, en la que f representa una asociación de Z_p a Z_q, y después genera una clave de grupo $K = g^{Fov}$ en función del exponente secreto v.

104: Después de recibir el mensaje intermedio difundido por el organizador, cada miembro del grupo extrae el exponente secreto y genera una clave de grupo en función del exponente secreto y del valor DH público de cada miembro.

Después de recibir M_i, todos los miembros U_i del grupo descrifran el valor v, y calculan la función $F = f(g^{r_2}, g^{r_3}, \cdots, g^{r_n})$, en la que f representa una asociación de Z_p a Z_q. A continuación, los miembros U_i del grupo calculan una clave de grupo $K = g^{Fov}$, en la que el símbolo ◦ indica que F y v se operan matemáticamente y su resultado tiene que ser módulo p.

Mediante los pasos descritos más arriba, las claves de grupo calculadas por todos los miembros U_i del grupo son las

mismas, esto es, la clave de grupo $K = g^{Fou}$.

Cuando un miembro se une al grupo o sale de él, es necesario volver a generar una clave de grupo de acuerdo con todos los miembros actuales del grupo después del cambio de miembros el grupo, en relación con la cual el proceso de cálculo es parecido al proceso de más arriba y no se repetirá de nuevo en la presente solicitud.

En la implementación de la presente invención, los inventores observan que la solución de negociación de la clave de grupo de la red Ad Hoc necesita una gran cantidad de cálculo, y por lo tanto tiene una baja velocidad de procesamiento, un gran espacio de almacenamiento y un requisito de gran ancho de banda.

El documento de Li, D. y Sampalli, S. “An Efficient Group Key Establishment In Location-Aided mobile ad hoc Networks (Un Establecimiento De Clave De Grupo Eficiente En Redes ad hoc móviles Asistidas por Localización)”, ACM, 2005, páginas 57-64 describe dos algoritmos de correspondencia máxima escalables (M2) para desarrollar en MANET acuerdos de clave de grupo basados en árboles binarios. Además, la técnica propuesta es ligera debido a que utiliza el intercambio de claves de Diffie-Hellman de Curva Elíptica en lugar del Diffie-Hellman normal y tampoco necesita soporte de terceras partes.

El documento XP002667535 divulga citas del Handbook of Applied Cryptography (Manual de Criptografía Aplicada) (Menezes, Vanstone, Oorschot, EE.UU., 1997) y en particular la generación de una clave de grupo mediante la técnica de Diffie Hellmann aplicada a tres o más partes, cuya funcionalidad forma una estructura en forma de estrella.

Resumen de la invención

Para reducir la cantidad de cálculo y el espacio de almacenamiento utilizado, y un menor requisito de ancho de banda de la solución de negociación de la clave de grupo, la presente invención proporciona un método, un sistema y dispositivos para generar una clave de grupo. A continuación se describen las soluciones técnicas.

Como un primer aspecto de la invención, el método para generar una clave de grupo selecciona parámetros del sistema en función de una curva elíptica, y en las respectivas formas de implementación del método se llevan a cabo los siguientes pasos.

Los miembros del grupo forman una estructura con forma de estrella y seleccionan un organizador entre los miembros del grupo.

Los miembros del grupo seleccionan individualmente de forma aleatoria valores DH secretos en función de los parámetros del sistema, generan individualmente valores DH públicos en función de los parámetros del sistema y de los valores DH secretos seleccionados y difunden en el grupo los valores DH públicos.

Después de recibir los valores DH públicos del resto de miembros del grupo, el organizador selecciona un exponente secreto, calcula un valor DH del mensaje intermedio en función del exponente secreto, genera un mensaje intermedio que incluye el valor DH del mensaje intermedio, difunde en el grupo el mensaje intermedio y genera una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos del resto de miembros del grupo.

Después de recibir el mensaje intermedio y un valor DH público del organizador, el resto de miembros del grupo calculan el valor DH secreto seleccionado por el organizador en función del mensaje intermedio, verifican que sea correcto el valor DH secreto calculado seleccionado por el organizador en función del valor DH público del organizador y genera una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos del resto de miembros del grupo.

Como un segundo aspecto de la invención el sistema para generar una clave de grupo incluye un dispositivo de comunicación que tiene el papel de organizador y dispositivos de comunicación que tienen el papel de miembros. En las respectivas formas de implementación se realizan las siguientes características.

El dispositivo de comunicación que tiene el papel de organizador está configurado para seleccionar un valor DH secreto en función de los parámetros del sistema, generar un valor DH público en función de los parámetros del sistema y del valor DH secreto seleccionado y difundir en el grupo el valor DH público; y después de recibir los valores DH públicos del resto de dispositivos, el dispositivo de comunicación que tiene el papel de organizador está configurado, además, para seleccionar un exponente secreto, calcular un valor DH del mensaje intermedio en función del exponente secreto, generar un mensaje intermedio que incluya el valor DH del mensaje intermedio, difundir en el grupo el mensaje intermedio, y generar una clave de grupo en función del valor DH secreto seleccionado y los valores DH públicos de todos los dispositivos del grupo.

Los dispositivos de comunicación que tienen el papel de miembros están configurados para seleccionar valores DH secretos en función de los parámetros del sistema, generar valores DH públicos en función de los parámetros del

sistema y de los valores DH secretos seleccionados y difundir los valores DH públicos; y después de recibir el valor DH público y el mensaje intermedio difundido por el dispositivo de comunicación que tiene el papel de organizador, los dispositivos de comunicación que tienen el papel de miembros están configurados, además, para calcular el valor DH secreto seleccionado por el organizador en función del mensaje intermedio, verificar que sea correcto el valor DH secreto calculado seleccionado por el organizador, y a continuación generar una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de todos los dispositivos del grupo.

Además, como un tercer aspecto de la invención, el dispositivo de comunicación incluye un módulo de selección de parámetros del sistema, un módulo de generación y difusión del valor DH público, un módulo de generación y difusión del mensaje intermedio y un módulo de generación de la clave de grupo del organizador. En las respectivas formas de implementación del dispositivo se realizan las siguientes características.

El módulo de selección de parámetros del sistema está configurado para seleccionar parámetros del sistema a partir de una curva elíptica.

El módulo de generación y difusión del valor DH público está configurado para seleccionar un valor DH secreto en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, generar un valor DH público en función de los parámetros del sistema y del valor DH secreto seleccionado y difundir el valor DH público.

El módulo de generación y difusión del mensaje intermedio está configurado para seleccionar un exponente secreto después de recibir los valores DH públicos difundidos por otros dispositivos de comunicación, calcular un valor DH del mensaje intermedio en función del exponente secreto, generar un mensaje intermedio que incluya el valor DH del mensaje intermedio en función del valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público, y difundir el mensaje intermedio.

El módulo de generación de la clave de grupo del organizador está configurado para recibir los valores DH públicos difundidos por otros dispositivos de comunicación, y generar una clave de grupo en función del valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público y los valores DH públicos difundidos por otros dispositivos de comunicación.

Como un cuarto aspecto de la invención, el dispositivo de comunicación incluye un módulo de selección de parámetros del sistema, un módulo de generación y difusión del valor DH público, y un módulo de generación de la clave de grupo del miembro. En las respectivas formas de implementación del dispositivo se realizan las siguientes características.

El módulo de selección de parámetros del sistema está configurado para seleccionar parámetros del sistema a partir de una curva elíptica.

El módulo de generación y difusión del valor DH público está configurado para seleccionar valores DH secretos en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, generar valores DH públicos en función de los parámetros del sistema y de los valores DH secretos seleccionados y difundir los valores DH públicos.

El módulo de generación de la clave de grupo del miembro está configurado para recibir un valor DH público y un mensaje intermedio difundido por otro dispositivo de comunicación, calcular un valor DH secreto seleccionado por un organizador en función del mensaje intermedio, verificar que sea correcto el valor DH secreto calculado seleccionado por el organizador en función del valor DH público difundido por el dispositivo de comunicación que difunde el mensaje intermedio, y generar una clave de grupo en función del valor DH secreto seleccionado por el organizador y de valores DH públicos difundidos por el resto de dispositivos de comunicación excepto el dispositivo de comunicación que difunde el mensaje intermedio.

Las soluciones técnicas de la presente invención se basan en un sistema de cifrado de curva elíptica, en el que un organizador transmite de forma segura al resto de miembros del grupo un exponente secreto a través de un valor DH del mensaje intermedio compartido con el resto de miembros del grupo y a continuación todos los miembros llevan a cabo la negociación basándose en la técnica de cifrado de clave pública sobre una curva elíptica para obtener una clave de grupo. Comparadas con las de la técnica anterior, las soluciones técnicas de la presente invención tienen las siguientes ventajas: una alta velocidad de cálculo, un reducido espacio de almacenamiento y un bajo requisito de ancho de banda de red, manteniendo la misma seguridad.

Breve descripción de los dibujos

La FIG. 1 es un diagrama de flujo de un método para generar una clave de grupo en la técnica anterior;

la FIG. 2 es un diagrama de flujo de un método para generar una clave de grupo de acuerdo con el Modo de realización 1 de la presente invención;

la FIG. 3 es una vista esquemática de una estructura con forma de estrella constituida por miembros del grupo de acuerdo con el Modo de realización 1 de la presente invención;

la FIG. 4 es una vista esquemática de una estructura con forma de estrella constituida por miembros del grupo cuando se incorporan nuevos miembros al grupo de acuerdo con el Modo de realización 2 de la presente invención;

la FIG. 5 es un diagrama de flujo de un método para generar una clave de grupo cuando se incorporan nuevos miembros al grupo de acuerdo con el Modo de realización 2 de la presente invención;

la FIG. 6 es una vista esquemática de una estructura con forma de estrella incorporan por miembros del grupo cuando se combinan grupos de acuerdo con el Modo de realización 3 de la presente invención;

la FIG. 7 es un diagrama de flujo de un método para generar una clave de grupo cuando se combinan grupos de acuerdo con el Modo de realización 3 de la presente invención;

la FIG. 8 es una vista de la estructura de un sistema para generar una clave de grupo de acuerdo con el Modo de realización 6 de la presente invención;

la FIG. 9 es una vista de la estructura de un dispositivo de comunicación de acuerdo con el Modo de realización 7 de la presente invención; y

la FIG. 10 es una vista de la estructura de otro dispositivo de comunicación de acuerdo con el Modo de realización 8 de la presente invención.

Descripción detallada de los modos de realización

Para hacer más comprensibles los objetos, soluciones técnicas y ventajas de la presente invención, a continuación se describen más en detalle algunos modos de realización de la presente invención haciendo referencia a los dibujos adjuntos.

Los modos de realización de la presente invención proporcionan un método, un sistema y un dispositivo para generar una clave de grupo, los cuales son aplicables a una red Ad Hoc. Específicamente, los miembros del grupo constituyen una estructura con forma de estrella, y se selecciona un miembro para que sea un organizador, el cual es responsable de transmitir de forma segura un exponente secreto al resto de miembros del grupo a través de un valor DH del mensaje intermedio compartido con el resto de miembros del grupo y, a continuación, para obtener una clave de grupo todos los miembros negocian basándose en la técnica de cifrado de clave pública sobre una curva elíptica. El valor DH del mensaje intermedio es un parámetro obtenido en función de un protocolo de negociación de claves de Diffie-Hellman (brevemente denominado como un protocolo de negociación de claves DH) sobre la curva elíptica.

Los modos de realización de la presente invención se basan en un sistema de cifrado de curva elíptica. El cifrado de curva elíptica (ECC) fue establecido por primera vez por Neal Koblitz y Victor Miller en el año 1985. El sistema de cifrado de curva elíptica tiene las siguientes ventajas: alta seguridad, baja carga de cálculo, pequeña longitud de clave, alta velocidad de procesamiento, pequeño espacio de almacenamiento ocupado, pequeño requisito de ancho de banda, etc., por lo que tiene un amplio potencial de aplicación en el campo de la seguridad. Recientemente, el sistema de cifrado de curva elíptica ha sido aceptado como un estándar por parte de las organizaciones de estandarización, como por ejemplo el Instituto de Estándares Nacional de América (ANSI), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), la Organización de Estandarización Internacional (ISO), y el Instituto Nacional de Estándares y Tecnología (NIST).

Modo de realización 1

La FIG. 2 es un diagrama de flujo de un método para generar una clave de grupo de acuerdo con un modo de realización de la presente invención. Haciendo referencia a la FIG. 2, el método incluye:

201: Los miembros de grupo U_1, …, U_n constituyen una estructura con forma de estrella y se selecciona un organizador.

De acuerdo con el modo de realización de la presente invención, n representa el número de miembros del grupo, y U_i representa un miembro del grupo con un número de secuencia i (i = 1, 2, …, n). Un miembro del grupo es seleccionado como organizador y en este modo de realización se selecciona como organizador a U_1. El organizador no es confiable, pero es temporal, y su papel lo puede realizar cualquier miembro. La FIG. 3 es una vista esquemática de una estructura con forma de estrella constituida por los miembros del grupo.

202: Se seleccionan los parámetros del sistema y se lleva a cabo la inicialización del sistema. A continuación se describe el proceso específico.

GF(p) es un campo finito con orden un número primo *p*, y una curva elíptica *EC:* se define en el campo $y^2=x^3+ax+ ß$ *(a, ß∈GF(p),* $4a^3+27\ ß^2$(mod *p*) ≠0; y *p* es un número primo grande de más de 190 bits). EC_p (*a, ß*) = {(*x,y*) | $y^2=x^3+ax+ ß$(mod *p*) } U *O* (*O* es la identidad) forma un grupo abeliano – grupo conmutativo.

En relación a un sistema ECC dado, se selecciona un punto $P∈EC_p$ (α, *ß*) como un punto base público, y el orden de *P* es un número primo grande *q* (en general, *q* ≥ 120 bits). Se define *G* = {*O, P, 2P, …,* (*q*-1)*P*}. De este modo, se puede saber que *G* es un grupo abeliano cíclico finito, y *q* es un período cíclico.

203: Un miembro U_i del grupo selecciona un valor DH secreto $r_i ∈ Z_q$, en función de los parámetros del sistema, genera un valor DH público $X_i = (x_i,y_i) = r_iP$ en función del valor DH secreto r_i y el punto base público *P,* y difunde en el grupo el valor DH público $X_i = (x_i,y_i) = r_iP$, en el que *i* tiene el valor de 1, …, n.

204: Después de recibir los valores DH públicos X_i difundidos por el resto de miembros, el organizador U_1 selecciona de forma aleatoria un exponente secreto $z ∈ Z_q$ (Z_q es un conjunto de restos no negativos mínimos obtenidos después de la operación módulo *q*, y *q* es un número primo perteneciente a los parámetros del sistema), calcula un valor DH del mensaje intermedio *zP* = (*x, y*) de acuerdo con el protocolo de negociación de claves Diffie-Hellman sobre la Curva Elíptica, genera un mensaje intermedio {$c_1, c_2, …, c_n$} = {r_1x(mod *p*), $r_2zP, r_3zP, …, r_nzP$}, en el que *p* es un número primo perteneciente a los parámetros del sistema, en función de los valores DH públicos recibidos del resto de miembros, el exponente *z* secreto seleccionado, el valor DH secreto r_1, y la coordenada x del valor DH del mensaje intermedio *zP*, difunde en el grupo el mensaje intermedio {$c_1, c_2, …, c_n$} = {r_1x(mod *p*), $r_2zP, r_3zP, …, r_nzP$}; genera una clave de grupo $K = r_1(r_2P + r_3P + … + r_nP)$ en función del valor DH secreto r_1 seleccionado por el propio organizador y los valores DH públicos del resto de miembros.

Se debe observar que, en este modo de realización, el mensaje intermedio también se puede generar en función de los valores DH públicos recibidos del resto de miembros, el exponente *z* secreto seleccionado, el valor DH secreto r_1, y la coordenada y del valor DH *zP* del mensaje intermedio. El principio específico es parecido al de generación del mensaje intermedio en función de los valores DH públicos recibidos del resto de miembros, el exponente *z* secreto seleccionado, el valor DH secreto r_1, y la coordenada x del valor DH *zP* del mensaje intermedio y no se repetirá en la presente solicitud.

205: Después de recibir el mensaje intermedio difundido por el organizador U_1, el miembro U_i del grupo (*i* puede ser 2, 3, …, *n*) extrae el valor DH del mensaje intermedio que se encuentra en el mensaje intermedio, en el que el valor DH *zP* del mensaje intermedio se obtiene de forma específica calculando $zP = (x,y) = r_i^{-1}c_i$, y a continuación, se obtiene la *x* en función del valor DH del mensaje intermedio *zP* = (*x, y*). Como $c_1 = r_1x$(mod *p*), se calcula $r_1 = c_1x^{-1}$ (mod *p*), siendo r_1 el valor DH secreto seleccionado por el organizador.

206: Después de calcular el valor DH secreto r_1 seleccionado por el organizador, el miembro U_i del grupo (*i* puede ser 2, 3, …, *n*) verifica si se cumple o no una ecuación $r_1P = X_1$, si se cumple se ejecuta el paso 207; en caso contrario se vuelve a ejecutar el paso 203.

La verificación de la ecuación $r_1P = X_1$ tiene el objetivo de verificar si se ha alterado o no el valor DH secreto seleccionado por el organizador.

207: El miembro U_i del grupo (*i* puede ser 2, 3, …, *n*) genera una clave de grupo $K = r_1(r_2P + r_3P + … + r_nP)$ en función del valor DH secreto seleccionado por el organizador y los valores DH públicos del resto de miembros del grupo excepto el organizador.

Mediante el proceso anterior, las claves de grupo calculadas por todos los miembros U_i del grupo son iguales, esto es, la clave de grupo $K = r_1(r_2P + r_3P + … + r_nP)$, y todos los miembros reservan los valores X_i recibidos en la etapa de negociación de clave.

Modo de realización 2

En este modo de realización se proporciona un método para generar una clave de grupo mediante negociación cuando se incorporan nuevos miembros al grupo. Este modo de realización se basa en el Modo de realización 1. Se asume que el grupo ∑ = {U_1, U_2, …, U_n} ha llevado a cabo la negociación básica del Modo de realización 1, y ha obtenido la clave de grupo compartida $K = r_1(r_2P + r_3P + … + r_nP)$. Ahora, *t* miembros pretenden unirse al grupo ∑, los cuales se representan, respectivamente, como U_{n+1}, U_{n+2}, …, U_{n+t}. El proceso de negociación para una nueva clave requiere que participen los *t* miembros recién incorporados y el organizador U_1. Haciendo referencia a la FIG. 4, U_1, U_2, …, U_{n+t} constituyen conjuntamente una estructura con forma de estrella.

La FIG. 5 es un diagrama de flujo de un método para generar una clave de grupo cuando se incorporan nuevos miembros al grupo. Haciendo referencia a la FIG. 5, el método para generar una clave de grupo cuando se incorporan nuevos miembros al grupo incluye:

301: El organizador U_1 y el nuevo miembro U_i seleccionan valores DH secretos $r_i' ∈ Z_q$ en función de los parámetros

del sistema, generan valores DH públicos $X_i' = (x_i', y_i') = r_i'P$ en función de los valores DH secretos r_i' y el punto base público *P*, y difunden en el grupo los valores DH públicos $X_i' = (x_i', y_i') = r_i'P$, en donde *i* puede ser *n*+1, …, *n*+*t*.

302: Después de recibir los valores DH públicos X_i' difundidos por los nuevos miembros, suponiendo que un exponente secreto *z'* = x_k, el organizador U_1 calcula un valor DH del mensaje intermedio *z'P* = (*x', y'*) de acuerdo con el protocolo de negociación de claves de Diffie-Hellman sobre la Curva Elíptica, genera un mensaje intermedio $\{c_1', c_{n+1}', \ldots, c_{n+t}'\} = \{r_1'x' \pmod p, r_{n+1}'z'P, r_{n+2}'z'P, \ldots, r_{n+t}'z'P\}$ que incluye el valor DH del mensaje intermedio, difunde en el grupo el mensaje intermedio $\{c_1', c_{n+1}', \ldots, c_{n+t}'\} = \{r_1'x' \pmod p, r_{n+1}'z'P, r_{n+2}'z'P, \ldots, r_{n+t}'z'P\}$, y genera una nueva clave de grupo $K' = r_1'(r_{n+1}'P, +r_{n+2}'P + \cdots + r_{n+t}'P)$ en función del valor DH secreto r_1' seleccionado por el propio organizador y los valores DH públicos de los nuevos miembros.

En este modo de realización, x_k representa una coordenada x de la clave *K* compartida por ∑ = {U_1, U_2, …, U_n}, y todos los miembros del grupo saben que el organizador U_1 selecciona la coordenada x o la coordenada y como *z'* con antelación. El organizador U_1 selecciona la coordenada x como *z'*, y también se puede suponer que *z'* = y_K, esto es, el organizador U_1 selecciona la coordenada y como *z'*.

303: Después de recibir el mensaje intermedio $\{c_1', c_{n+1}', \ldots, c_{n+t}'\} = \{r_1'x' \pmod p, r_{n+1}'z'P, r_{n+2}'z'P, \ldots, r_{n+t}'z'P\}$ difundido por el organizador U_1, el nuevo miembro U_i (*i*∈{*n*+1, …, *n*+*t*}) extrae el valor DH del mensaje intermedio incluido en el mensaje intermedio, en donde el valor DH del mensaje intermedio *z'P* se obtiene específicamente calculando $z'P = (x', y') = r_i'^{-1}c_i'$ y, a continuación se obtiene *x'* en función del valor DH del mensaje intermedio *z'P* = (*x', y'*). Como $c_1' = r_1'x' \pmod p$, se calcula $r_1' = c_1'x'^{-1} \pmod p$, siendo r_1' el valor DH secreto seleccionado por el organizador.

304: Después de calcular el valor DH secreto r_1' seleccionado por el organizador, el nuevo miembro U_i (*i*∈{*n*+1, …, *n*+*t*}) verifica si se satisface o no la ecuación $r_1'P = X_1'$, si lo hace, se ejecuta el paso 305; en caso contrario, se vuelve a ejecutar el paso 301.

La verificación de la ecuación $r_1'P = X_1'$ tiene el objetivo de verificar si se ha alterado o no el valor DH secreto seleccionado por el organizador.

305: El nuevo miembro U_i (*i*∈{*n*+1, …, *n*+*t*}) genera una nueva clave de grupo $K' = r_1'(r_{n+1}'P + r_{n+2}'P + \cdots + r_{n+t}'P)$ en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de los nuevos miembros.

306: Los otros miembros U_2, …, U_n del grupo ∑ obtienen *z'* = x_K en función del valor de z anterior, calculan $z'P = (x', y') = r_i'^{-1}c_i'$, (*i*∈{2, …, *n*}) y a continuación obtienen *x'* en función del valor DH del mensaje intermedio *z'P* = (*x', y'*). Como $c_1' = r_1'x' \pmod p$, se calcula $r_1' = c_1'x'^{-1} \pmod p$, siendo r_1' el valor DH secreto seleccionado por el organizador. A continuación, en función del valor DH secreto r_1' seleccionado por el organizador y los valores DH públicos de los nuevos miembros, cada uno de los otros miembros U_2, …, U_n genera una nueva clave de grupo $K' = r_1'(r_{n+1}'P + r_{n+2}'P + \cdots + r_{n+t}'P)$.

Mediante el proceso anterior, después de que los *t* miembros se hayan incorporado al grupo ∑, cada miembro U_i del grupo (*i*∈{1, …, *n*+*t*}) calcula una nueva clave de grupo $K' = r_1'(r_{n+1}'P + r_{n+2}'P + \cdots + r_{n+t}'P)$, y los *t* miembros recién añadidos reservan los valores X_i' recibidos en la etapa de negociación de clave.

Por ejemplo, se asume que un grupo ∑ = {U_1, …, U_5} ha realizado la negociación básica y ha obtenido la clave compartida $K = r_1(r_2P + r_3P + \ldots + r_5P)$. Un miembro *G'* = {$U_6$} tiene que incorporarse al grupo y comparte una nueva clave con los miembros del grupo ∑. De acuerdo con el método de este modo de realización, el proceso de negociación de clave requiere que U_1 interactúe con el miembro U_6 recién incorporado de modo que todos los miembros del grupo puedan calcular y obtener la nueva clave de grupo. En este ejemplo, después de que U_1, U_2, …, U_6 constituyan conjuntamente una estructura con forma de estrella, se ejecutan los siguientes pasos específicos.

(1) El organizador U_1 selecciona el valor DH secreto $r_1' \in Z_q$ en función de los parámetros del sistema, y envía a U_6 el mensaje $X_1' = (x_1', y_1') = r_1'P$. U_6 selecciona el valor DH secreto $r_6' \in Z_q$ en función de los parámetros del sistema, y envía a U_1 el mensaje $X_6' = (x_6', y_6') = r_6'P$.

(2) Después de recibir el valor DH público X_6' enviado por U_6, suponiendo que un exponente secreto *z'* = x_K, el organizador U_1 calcula un valor DH del mensaje intermedio *z'P* = (*x', y'*) de acuerdo con el protocolo de negociación de claves de Diffie-Hellman sobre la Curva Elíptica, genera un mensaje intermedio $\{c_1', c_6'\} = \{r_1'x' \pmod p, r_6'z'P\}$ que incluye el valor DH del mensaje intermedio, difunde en el grupo el mensaje intermedio $\{c_1', c_6'\} = \{r_1'x' \pmod p, r_6'z'P\}$, y genera una clave de grupo $K' = r_1'r_6'P$ en función del valor DH secreto r_1' seleccionado por el propio organizador y el valor DH público de U_6.

En el ejemplo, x_K representa una coordenada x de la clave *K* compartida por ∑ = {U_1, U_2, …, U_5}.

(3) Después de recibir el mensaje intermedio difundido por el organizador U_1, U_6 extrae el valor DH del mensaje intermedio incluido en el mensaje intermedio, en donde el valor DH del mensaje intermedio *z'P* se obtiene específicamente calculando $z'P = (x', y') = r_6'^{-1}c_6'$ y, a continuación se obtiene *x'* en función del valor DH del mensaje intermedio *z'P* = (*x', y'*). Como $c_1' = r_1'x' (\mathrm{mod}\ p)$, se calcula $r_1' = c_1'x'^{-1} (\mathrm{mod}\ p)$, siendo r_1' el valor DH secreto seleccionado por el organizador U_1.

(4) Después de calcular el valor DH secreto r_1' seleccionado por el organizador U_1, U_6 verifica si se satisface o no la ecuación $r_1'P = X_1'$, si lo hace, se ejecuta el paso (5); en caso contrario, se vuelve a ejecutar el paso (1).

La verificación de la ecuación $r_1'P = X_1'$ tiene el objetivo de verificar si se ha alterado o no el valor DH secreto seleccionado por el organizador.

(5) U_6 genera una clave de grupo $K' = r_1'r_6'P$ en función del valor DH secreto r_1' seleccionado por el organizador U_1 y el valor DH público de U_6.

(6) Los otros miembros U_2, …, U_5 en el grupo $\sum$ obtienen *z'* = x_K en función del valor de z anterior, calculan $z'P = (x', y') = r_i'^{-1}c_i'$, (*i*∈{2, …, *5*}) y obtienen la *x'* en función del valor DH del mensaje intermedio *z'P* = (*x', y'*). Como $c_1' = r_1'x' (\mathrm{mod}\ p)$, se calcula $r_1' = c_1'x'^{-1} (\mathrm{mod}\ p)$, siendo r_1' el valor DH secreto seleccionado por el organizador. Después, en función del valor DH secreto r_1' seleccionado por el organizador U_1 y el valor DH público del nuevo miembro U_6, cada uno de los otros miembros U_2, …, U_5 genera una clave de grupo $K' = r_1'r_6'P$.

Mediante el método anterior, todos los miembros obtienen la misma clave de grupo $K' = r_1'r_6'P$.

Modo de realización 3

En este modo de realización se proporciona un método para generar una clave de grupo mediante negociación cuando se combinan grupos. Este modo de realización se basa en el Modo de realización 1. Se necesitan combinar *t* grupos, los cuales se representan como $\{\sum_1, \sum_2, \ldots, \sum_t\}$ respectivamente, y cada grupo $\sum_i$ tiene n_i miembros, esto es, $\sum_i = \{U_{i1}, U_{i2}, \ldots, U_{in_i}\}$ (i∈{1, *t*}). Cada grupo ha realizado, respectivamente, la negociación básica del Modo de realización 1, y los miembros del grupo $\sum_i$ comparten una clave de grupo K_i. En la presente solicitud se selecciona U_{11} como un nuevo organizador, $\sum_1$ es un grupo de combinación principal, y $\sum_2, \ldots, \sum_t$ son grupos de combinación secundarios. El proceso de negociación requiere que participe el organizador U_{i1} de cada grupo $\sum_i$. Haciendo referencia a la FIG. 6, los grupos a combinar se constituyen conjuntamente en una estructura con forma de estrella y, haciendo referencia a la FIG. 7, a continuación se describe el proceso de negociación de clave.

401: U_{11} selecciona un valor DH secreto $r_{11}' \in Z_q$ en función de los parámetros del sistema, genera un valor DH público $X_{11}' = (x_{11}', y_{11}') = r_{11}'P$ en función del valor DH secreto r_{11}' y un punto base público *P*, y difunde en el grupo el valor DH público $X_{11}' = (x_{11}', y_{11}') = r_{11}'P$.

402: Suponiendo que un valor DH secreto $r_{i1}' = x_{K_i}$, el organizador U_{i1} de cada uno de los grupos $\sum_2, \ldots, \sum_t$ de combinación secundarios genera un valor DH público $X_{i1}' = (x_{i1}', y_{i1}') = r_{i1}'P$ en función del valor DH secreto r_{i1}' y el punto base público *P*, y difunde en el grupo el valor DH público $X_{i1}' = (x_{i1}', y_{i1}') = r_{i1}'P$, donde *i* tiene el valor de 2, …, *t*.

En el modo de realización, x_{K_i} representa una coordenada x de la clave K_i compartida en el $\sum_i = \{U_{i1}, U_{i2}, \ldots, U_{in_i}\}$ (i∈{1, *t*}), y todos los miembros del grupo saben que el organizador U_{i1} selecciona la coordenada x o la coordenada y como *z'* con antelación. En este modo de realización, el organizador U_{i1} selecciona la coordenada x como *z'*, y también se puede suponer que $z' = y_{K_i}$, esto es, el organizador U_{i1} selecciona la coordenada y como *z*'.

403: Después de recibir los valores DH públicos X_{i1}' difundidos por U_{i1}, suponiendo que un exponente secreto $z' = y_{K_i}$, U_{11} calcula un valor DH del mensaje intermedio *z'P* = (*x', y'*) basándose en el protocolo de negociación de claves de Diffie-Hellman sobre la Curva Elíptica, genera un mensaje intermedio $\{c_1', c_2', \ldots, c_t'\} = \{r_{11}'x' (\mathrm{mod}\ p), r_{21}'z'P, r_{31}'z'P, \ldots, r_{t1}'z'P\}$ que incluye el valor DH del mensaje intermedio, difunde en el grupo el mensaje intermedio $\{c_1', c_2', \ldots, c_t'\} = \{r_{11}'x' (\mathrm{mod}\ p), r_{21}'z'P, r_{31}'z'P, \ldots, r_{t1}'z'P\}$, y genera una nueva clave de grupo $K' = r_{11}'(r_{21}'P + r_{31}'P + \cdots + r_{t1}'P)$ en función del valor DH secreto r_{11}' seleccionado por el propio U_{11} y el valor DH público de U_{i1}.

404: Después de recibir el mensaje intermedio difundido por U_{11}, U_{i1} (*i*∈{2, …, *t*}) extrae el valor DH del mensaje intermedio incluido en el mensaje intermedio, en donde el valor DH del mensaje intermedio *z'P* se obtiene específicamente calculando $z'P = (x', y') = r_{i1}'^{-1}c_i'$ y, a continuación se obtiene *x'* en función del valor DH del mensaje intermedio *z'P* = (*x', y'*). Como $c_1' = r_{11}'x' (\mathrm{mod}\ p)$, se calcula $r_{i1}' = c_1'x'^{-1} (\mathrm{mod}\ p)$, siendo r_{11}' el valor DH secreto seleccionado por el organizador.

405: Después de calcular el valor DH secreto r'_{11} seleccionado por U_{11}, U_{i1} (i∈{2, …, t}) verifica si se satisface o no la ecuación $r'_{11}P = X'_{11}$, si lo hace, se ejecuta el paso 406; en caso contrario, se vuelve a ejecutar el paso 401.

La verificación de la ecuación $r'_{11}P = X'_{11}$ tiene el objetivo de verificar si se ha alterado o no el valor DH secreto seleccionado por el organizador U_{11}.

406: U_{i1} (i∈{2, …, t}) genera una nueva clave de grupo $K' = r'_{11}(r'_{21}P + r'_{31}P + \cdots + r'_{t1}P)$ en función del valor DH secreto r'_{11} seleccionado por U_{11} y el valor DH público de U_{i1}.

407: El resto de miembros de los grupos $\sum_i$(i∈{2, …, t}) de combinación secundarios, excepto los organizadores, obtienen $z' = x_{K_1}$ en función del valor z anterior, calculan $z'P = (x', y') = r'^{-1}_{i1}c'_i$ (i∈{1, 2, …, t}), y obtienen x' en función del valor DH del mensaje intermedio $z'P = (x', y')$. Como $c'_1 = r'_{11}x' \pmod p$, se calcula $r'_{11} = c'_1 x'^{-1} \pmod p$, siendo r'_{11} el valor DH secreto seleccionado por el organizador. A continuación, en función del valor DH secreto r'_{11} seleccionado por U_{11} y el valor DH público de U_{i1}, cada uno de los otros miembros de los grupos $\sum_i$(i∈{2, …, t}) de combinación secundarios genera una nueva clave de grupo $K' = r'_{11}(r'_{21}P, + r'_{31}P + \cdots + r'_{t1}P)$.

408: En función del x_{K_1} obtenido con anterioridad, el resto de miembros del grupo $\sum_1$ de combinación principal excepto el organizador, calcula $z'P = (x', y') = r'^{-1}_{i1}c'_i$ (i∈{1, 2, …, t}), y a continuación obtienen la x' correspondiente en función del valor DH del mensaje intermedio $z'P = (x', y')$. Como $c'_1 = r'_{11}x' \pmod p$, se calcula $r'_{11} = c'_1 x'^{-1} \pmod p$, siendo r'_{11} el valor DH secreto seleccionado por el organizador. A continuación, en función del valor DH secreto r'_{11} seleccionado por U_{11} y el valor DH público de U_{i1}, cada uno de los otros miembros del grupo $\sum_1$ de combinación principal genera una nueva clave de grupo $K' = r'_{11}(r'_{21}P + r'_{31}P + \cdots + r'_{t1}P)$.

Mediante el método anterior, se combinan t grupos en un grupo siendo U_{11} el organizador, y todos los miembros comparten la clave de grupo $K' = r'_{11}(r'_{11}P + r'_{31}P + \cdots + r'_{t1}P)$.

Modo de realización 4

En este modo de realización, se proporciona un método para generar una clave de grupo cuando algunos miembros abandonan el grupo. Este modo de realización está basado en el Modo de realización 1. Se asume que los miembros del grupo $\sum = \{U_1, \ldots, U_n\}$ han realizado la negociación básica del Modo de realización 1. k miembros $\sum' = \{U_{j_1}, \ldots, U_{j_k}\}$ tienen que abandonar el grupo y los otros miembros del grupo $\sum'' = \{U_1, \ldots, U_{j_1-1}, U_{j_1+1}, \ldots, U_{j_k-1}, U_{j_k+1}, \ldots, U_n\}$ permanecen en el grupo. Los miembros del grupo restantes tienen que calcular una nueva clave de grupo para evitar que los miembros que han abandonado el grupo obtengan la clave de grupo del grupo actual y se llevan a cabo los siguientes pasos específicos.

Primero, después de que k miembros abandonen el grupo $\sum$, el organizador U_1, en función de los parámetros del sistema, vuelve a seleccionar el valor DH secreto r'_1, con z'∈Z_q, y los otros miembros en G'' no tienen que volver a seleccionar los valores DH secretos.

A continuación los otros miembros del grupo $\sum'' = \{U_1, \ldots, U_{j_1-1}, U_{j_1+1}, \ldots, U_{j_k-1}, U_{j_k+1}, \ldots, U_n\}$, llevan a cabo una vez más el método de negociación de clave de grupo del Modo de realización 1, generan un nuevo mensaje intermedio $\{c'_1, \ldots, c'_{j_1-1}, c'_{j_1+1}, \ldots, c'_{j_k-1}, c'_{j_k+1}, \ldots, c'_n\} = \{r'_1 x' \pmod p, \ldots, r'_{j_1-1}z''P, r'_{j_1+1}z'P, \ldots, r'_{j_k-1}z'P, r'_{j_k+1}z'P, \ldots, r'_n z'P\}$, y generan una nueva clave de grupo $K' = r'_1(r_2P + \cdots + r_{j_1-1}P + r_{j_1+1}P + r_{j_k-1}P + r_{j_k+1}P + \cdots + r_nP)$ para compartirla.

Si el organizador del grupo original $\sum$ ha abandonado el grupo, es necesario volver a seleccionar un miembro para que sea el organizador en el grupo G'', y a continuación ejecutar los pasos de más arriba para generar una nueva clave de grupo $K' = r''_1(r_2P + \cdots + r_{j_1-1}P + r_{j_1+1}P + r_{j_k-1}P + r_{j_k+1}P + \cdots + r_nP)$ para compartirla.

Modo de realización 5

A medida que la escala del grupo se amplía continuamente, la carga de cálculo y la carga de comunicaciones del organizador aumentan rápidamente. Cuando la escala de la red aumenta hasta un punto determinado, el rendimiento del organizador se convierte en un cuello de botella del protocolo de modo que es necesario modificar de forma apropiada el rendimiento del organizador y así reducir la carga del organizador.

En este modo de realización se proporciona un método de negociación de clave de grupo para la comunicación de grupos grandes. Este modo de realización se basa en el Modo de realización 1. Cuando es muy grande el número de miembros del grupo que participan en la negociación, los miembros del grupo $\sum$ se dividen en m subgrupos lo que se representa como $\sum = \{\sum_1, \sum_2, \ldots, \sum_m\}$, y todos los nodos se constituyen en una estructura con forma de estrella. Cada subgrupo $\sum_i$ tiene n_i miembros, lo que se representa como $\{U_{i1}, U_{i2}, \ldots, U_{in_i}\}$. Los n_i miembros también se pueden constituir en una estructura con forma de estrella y U_{i1} se convierte en un organizador del subgrupo $\sum_i$.

Como método para dividir el grupo, el grupo se puede dividir en función de un código de máquina único correspondiente a cada dispositivo del nodo (parecido a una dirección MAC de una tarjeta de red Ethernet), y también se puede dividir en función de localizaciones geográficas. Se llevan a cabo los siguientes pasos.

Primero, los n_i miembros del subgrupo $\sum_i$ (i=1, 2, …, m) constituyen una estructura con forma de estrella, y llevan a cabo la negociación básica del Modo de realización 1 con el fin de obtener una clave de grupo $K_i = r_{i1}(r_{i2}P + r_{i3}P + \ldots + r_{in_i}P)$.

A continuación, se selecciona el organizador U_{11} del subgrupo $\sum_1$ como un organizador del grupo $\sum$, y los organizadores U_{i1} de los subgrupos $\sum_i$, en representación de cada subgrupo, constituyen una estructura con forma de estrella junto con U_{11}, con el fin de llevar a cabo una vez más la negociación básica del Modo de realización 1.

U_{11} vuelve a seleccionar un valor DH secreto $r'_{11} \in Z_q$, genera un valor DH público $X'_{11} = (x'_{11}, y'_{11}) = r'_{11}P$ en función del valor DH secreto r'_{11} y el punto base público P, y difunde en el grupo el valor DH público $X'_{11} = (x'_{11}, y'_{11}) = r'_{11}P$.

U_{i1} ($i \in \{1, 2, \ldots, n\}$) participa en el cálculo tomando la coordenada x x_{K_i} de la clave K_i de grupo individual, esto es x_{K_i}, como un valor DH secreto, genera un valor DH público $X'_{i1} = (x'_{i1}, y'_{i1}) = x_{K_i}P$ en función del valor DH secreto x_{K_i} y el punto base público P, y difunde en el grupo el valor DH público $X'_{i1} = (x'_{i1}, y'_{i1}) = x_{K_i}P$.

U_{11} toma la coordenada x x_{K_1} del valor de la clave K_1 del subgrupo $\sum_1$, esto es x_{K_1}, como un nuevo exponente secreto $z' = x_{K_1}$, calcula un valor DH del mensaje intermedio $z'P = (x', y')$ basándose en el protocolo de negociación de claves de Diffie-Hellman sobre la Curva Elíptica, genera un mensaje intermedio $\{c'_1, c'_2, \ldots, c'_n\} = \{r'_{11}x' (\mathrm{mod}\ p), x_{K_2}P, x_{K_3}P, \ldots, x_{K_m}P\}$ que incluye el valor DH del mensaje intermedio, difunde en el grupo el mensaje intermedio $\{c'_1, c'_2, \ldots, c'_n\} = \{r'_{11}x' (\mathrm{mod}\ p), x_{K_2}P, x_{K_3}P, \ldots, x_{K_m}P\}$, y genera una clave de grupo $K = r'_{11}(x_{K_2}P + x_{K_3}P + \cdots + x_{K_m}P)$ en función del valor DH secreto r'_{11} seleccionado por el propio U_{11} y el valor DH público recibido $X'_{i1} = (x'_{i1}, y'_{i1}) = x_{K_i}P$ difundido por los U_{i1}.

Después de recibir el mensaje intermedio difundido por el organizador U_{11}, U_{i1} ($i \in \{2, \ldots, m\}$) extrae el valor DH del mensaje intermedio incluido en el mensaje intermedio, en donde el valor DH del mensaje intermedio $z'P = (x', y')$ se obtiene específicamente calculando $z'P = (x', y') = x_{K_1}^{-1}c'_i$, y a continuación se obtiene x' en función del valor DH del mensaje intermedio $z'P = (x', y')$. Como $c'_1 = r'_{11}x' (\mathrm{mod}\ p)$, se calcula $r'_{11} = c'_1 x'^{-1} (\mathrm{mod}\ p)$, siendo r'_{11} el valor DH secreto seleccionado por el organizador U_{11}. U_{i1} genera una clave de grupo $K = r'_{11}(x_{K_2}P + x_{K_3}P + \cdots + x_{K_m}P)$ en función de r'_{11} y del valor DH público de U_{i1} ($i \in \{2, \ldots, m\}$).

Al mismo tiempo, los otros miembros U_{ij} ($i \in [1,m]$, $j \in [1,n_i]$) del grupo $\sum$ monitorizan el mensaje enviado al grupo $\sum_i$ correspondiente, obtienen x_{K_1} utilizando la clave K_i obtenida del subgrupo $\sum_i$, y calculan el valor DH secreto r'_{11} utilizando el mensaje intermedio difundido con el fin de obtener la clave de grupo compartida $K = r'_{11}(x_{K_2}P + x_{K_3}P + \cdots + x_{K_m}P)$.

Por último, todos los miembros obtienen la misma clave de grupo $K = r'_{11}\left(x_{K_2}P + x_{K_3}P + \cdots + x_{K_m}P\right)$.

Mediante el método anterior, el grupo $\sum$ se divide en m subgrupos = $\{\sum_1, \sum_2, \ldots, \sum_m\}$ para reducir la carga del organizador del grupo $\sum$, y todos los miembros del grupo $\sum$ comparten la clave de grupo $K = r'_{11}\left(x_{K_2}P + x_{K_3}P + \cdots + x_{K_m}P\right)$.

Modo de realización 6

Haciendo referencia a la FIG. 8, se proporciona un sistema para generar una clave de grupo. El sistema incluye un dispositivo de comunicación que tiene el papel de organizador y dispositivos de comunicación que tienen el papel de miembros.

El dispositivo de comunicación que tiene el papel de organizador está configurado para seleccionar un valor DH secreto en función de los parámetros del sistema, generar un valor DH público en función de los parámetros del sistema y del valor DH secreto seleccionado y difundir en el grupo el valor DH público; y después de recibir los valores DH públicos de otros dispositivos, el dispositivo de comunicación que tiene el papel de organizador está configurado, además, para seleccionar un exponente secreto, calcular un valor DH del mensaje intermedio en función del exponente secreto, generar un mensaje intermedio que incluya el valor DH del mensaje intermedio, difundir en el grupo el mensaje intermedio, y generar una clave de grupo en función del valor DH secreto seleccionado y los valores DH públicos de todos los dispositivos del grupo.

Los dispositivos de comunicación que tienen el papel de miembros están configurados para seleccionar valores DH secretos en función de los parámetros del sistema, generar valores DH públicos en función de los parámetros del

sistema y de los valores DH secretos seleccionados y difundir los valores DH públicos; y después de recibir el valor DH público y el mensaje intermedio difundido por el dispositivo de comunicación que tiene el papel de organizador, los dispositivos de comunicación que tienen el papel de miembros están configurados, además, para calcular el valor DH secreto seleccionado por el organizador en función del mensaje intermedio, verificar que sea correcto el valor DH secreto, y a continuación generar una clave de grupo en función del valor DH secreto y los valores DH públicos de todos los dispositivos del grupo.

Cuando se incorporan algunos miembros al grupo o lo abandonan, el dispositivo de comunicación que tiene el papel de organizador y los dispositivos de comunicación que tienen el papel de miembros en el sistema están configurados, además, para volver a generar y difundir nuevos valores DH públicos.

Modo de realización 7

Haciendo referencia a la FIG. 9, se proporciona un dispositivo de comunicación. El dispositivo incluye: un módulo de selección de parámetros del sistema, un módulo de generación y difusión del valor DH público, un módulo de generación y difusión del mensaje intermedio y un módulo de generación de la clave de grupo del organizador.

El módulo de selección de parámetros del sistema está configurado para seleccionar parámetros del sistema a partir de una curva elíptica.

El módulo de generación y difusión del valor DH público está configurado para seleccionar un valor DH secreto en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, generar un valor DH público en función de los parámetros del sistema y del valor DH secreto seleccionado y difundir el valor DH público.

El módulo de generación y difusión del mensaje intermedio está configurado para seleccionar un exponente secreto después de recibir los valores DH públicos difundidos por otros dispositivos de comunicación, calcular un valor DH del mensaje intermedio en función del exponente secreto, generar un mensaje intermedio que incluya el valor DH del mensaje intermedio en función del valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público, y difundir el mensaje intermedio.

El módulo de generación de la clave de grupo del organizador está configurado para recibir los valores DH públicos difundidos por otros dispositivos de comunicación, y generar una clave de grupo en función del valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público y los valores DH públicos difundidos por otros dispositivos de comunicación.

Con el objetivo de mejorar todavía más el dispositivo de comunicación, cuando algunos miembros se incorporan al grupo o lo abandonan, el dispositivo de comunicación incluye, además, un módulo de actualización de la clave de grupo.

El módulo de actualización de la clave de grupo está configurado para ordenar al módulo de generación y difusión del valor DH público que genere y difunda un nuevo valor DH público cuando se incorporen nuevos miembros al grupo o algunos lo abandonen.

A continuación se describe el proceso de generación de una nueva clave de grupo cuando nuevos miembros se incorporan al grupo.

El módulo de actualización de clave de grupo ordena al módulo de generación y difusión del valor DH público que seleccione un nuevo valor DH secreto para el organizador y los nuevos miembros en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, que genere un nuevo valor DH público en función de los parámetros del sistema y del nuevo valor DH secreto seleccionado, y que difunda el nuevo valor DH público.

El módulo de generación y difusión del mensaje intermedio selecciona un nuevo exponente secreto después de recibir los valores DH públicos de los nuevos miembros difundidos por otros dispositivos, calcula un nuevo valor DH del mensaje intermedio en función del nuevo exponente secreto, genera un nuevo mensaje intermedio que incluya el nuevo valor DH del mensaje intermedio en función del nuevo valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público, y difunde el nuevo mensaje intermedio.

El módulo de generación de la clave de grupo del organizador genera una nueva clave de grupo en función del nuevo valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público y los valores DH públicos recibidos de los nuevos miembros difundidos por otros dispositivos.

A continuación se describe el proceso de generación de una nueva clave de grupo cuando algunos miembros abandonan el grupo.

El módulo de actualización de la clave de grupo ordena al módulo de generación y difusión del valor DH público que

seleccione un nuevo valor DH secreto para el organizador en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, que genere un nuevo valor DH público en función de los parámetros del sistema y del nuevo valor DH secreto seleccionado, y que difunda el nuevo valor DH público.

El módulo de generación y difusión del mensaje intermedio selecciona un nuevo exponente secreto después de recibir los valores DH públicos de los miembros restantes difundidos por otros dispositivos, calcula un nuevo valor DH del mensaje intermedio en función del nuevo exponente secreto, genera un nuevo mensaje intermedio que incluya el nuevo valor DH del mensaje intermedio en función del nuevo valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público, y difunde el nuevo mensaje intermedio.

El módulo de generación de la clave de grupo del organizador genera una nueva clave de grupo en función del nuevo valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público y los valores DH públicos recibidos de los miembros restantes difundidos por otros dispositivos.

Modo de realización 8

Haciendo referencia a la FIG. 10, se proporciona otro dispositivo de comunicación. El dispositivo incluye: un módulo de selección de parámetros del sistema, un módulo de generación y difusión del valor DH público y un módulo de generación de la clave de grupo del miembro.

El módulo de selección de parámetros del sistema está configurado para seleccionar parámetros del sistema a partir de una curva elíptica.

El módulo de generación y difusión del valor DH público está configurado para seleccionar valores DH secretos en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, generar valores DH públicos en función de los parámetros del sistema y de los valores DH secretos seleccionados y difundir los valores DH públicos generados.

El módulo de generación de la clave de grupo del miembro está configurado para recibir valores DH públicos y un mensaje intermedio difundido por otro dispositivo de comunicación, calcular un valor DH secreto seleccionado por un organizador en función del mensaje intermedio, verificar que sea correcto el valor DH secreto en función del valor DH público difundido por el dispositivo de comunicación que difunde el mensaje intermedio, y generar una clave de grupo en función del valor DH secreto y de los valores DH públicos difundidos por el resto de dispositivos de comunicación excepto el dispositivo de comunicación que difunde el mensaje intermedio.

Con el objetivo de mejorar todavía más el dispositivo de comunicación, cuando algunos miembros se incorporan al grupo o lo abandonan, el dispositivo de comunicación incluye, además, un módulo de actualización de la clave de grupo.

El módulo de actualización de la clave de grupo está configurado para ordenar al módulo de generación y difusión del valor DH público que genere y difunda un nuevo valor DH público para los nuevos miembros incorporados cuando se incorporan al grupo nuevos miembros.

Cuando se incorporan al grupo nuevos miembros, el módulo de actualización de clave de grupo ordena al módulo de generación y difusión del valor DH público que seleccione nuevos valores DH secretos para los nuevos miembros en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, que genere nuevos valores DH públicos de los nuevos miembros en función de los parámetros del sistema y de los nuevos valores DH secretos seleccionados, y que difunda los nuevos valores DH públicos de los nuevos miembros. Después de recibir el nuevo mensaje intermedio, el módulo de generación de la clave de grupo del miembro calcula un nuevo valor DH secreto seleccionado por un organizador en función del nuevo mensaje intermedio, verifica que el nuevo valor DH secreto sea correcto en función del nuevo valor DH público recibido del organizador, y genera una nueva clave de grupo en función del nuevo valor DH secreto y los nuevos valores DH públicos de los nuevos miembros difundidos por el módulo de generación y difusión del valor DH público.

Cuando algunos miembros abandonan el grupo, después de recibir un nuevo mensaje intermedio, el módulo de generación de la clave de grupo del miembro calcula un nuevo valor DH secreto seleccionado por el organizador en función del nuevo mensaje intermedio, verifica que el nuevo valor DH secreto sea correcto en función del nuevo valor DH público recibido del organizador, y genera una nueva clave de grupo en función del nuevo valor DH secreto y de los nuevos valores DH públicos de los miembros restantes difundidos por el módulo de generación y difusión del valor DH público.

Los modos de realización descritos más arriba tienen las siguientes ventajas.

1) Alta seguridad: la complejidad de cálculo del problema del logaritmo discreto de la curva elíptica es, en la actualidad, de tipo exponencial, pero el sistema de cifrado de clave pública RSA es de tipo subexponencial.

2) Baja carga de cálculo y alta velocidad de proceso: bajo la misma condición de recursos de cálculo, el sistema de

cifrado de curva elíptica tiene una mayor velocidad de proceso si se compara con el RSA y el algoritmo de firma digital (DSA).

3) Pequeño espacio de almacenamiento: la longitud de clave y los parámetros del sistema del sistema de cifrado de curva elíptica son mucho menores que los del RSA y el DSA. El cifrado de curva elíptica (ECC) de 160 bits proporciona el mismo nivel de seguridad que el RSA o el DSA de 1024 bits y el ECC de 210 bits proporciona el mismo nivel de seguridad que el RSA o el DSA de 2048 bits, lo que significa que el sistema de cifrado de curva elíptica ocupa un espacio de almacenamiento mucho menor.

4) Bajo requisito de ancho de banda: para un nivel de seguridad dado, el ECC tiene un parámetro menor que el RSA y el DSA. La diferencia de tamaño de los parámetros del ECC y del RSA y el DSA es más obvia para un nivel de seguridad más alto. El parámetro de pequeño tamaño tiene ventajas de una alta velocidad de cálculo, una clave corta y un certificado de clave pequeño y, de este modo, la longitud de firma y la longitud del texto cifrado son también cortos.

Teniendo en cuenta lo anterior, el ECC puede proporcionar una alta seguridad con poca sobrecarga (por ejemplo, ancho de banda, carga de cálculo, espacio de almacenamiento y consumo de energía) y un pequeño retardo, lo cual es especialmente apropiado para la situación en la que la capacidad de cálculo y el ancho de banda están limitados como, por ejemplo, la comunicación de seguridad en un entrono de red Ad Hoc. Comparado con soluciones parecidas, cuando se proporciona el mismo nivel de seguridad, el ECC posee las ventajas de alta velocidad de cálculo, pequeño espacio de almacenamiento, un requisito bajo de ancho de banda de red, etc.

Los modos de realización de la presente invención soportan la incorporación y el abandono de miembros. Específicamente, cuando algunos miembros se incorporan al grupo, es necesario que los miembros recién incorporados y el organizador participen en la negociación y, cuando algunos miembros abandonan el grupo, el organizador debe volver a seleccionar un número aleatorio, sin necesidad de volver a seleccionar números aleatorios para los restantes miembros. Así pues, los modos de realización de la presente invención poseen una alta velocidad de cálculo, ocupan un pequeño espacio de almacenamiento y su utilización es flexible.

Cuando se aplica en la comunicación de grupos muy grandes, las soluciones técnicas de los modos de realización de la presente invención pueden reducir de forma efectiva la carga de cálculo del organizador al mismo tiempo que aumenta ligeramente la carga de comunicación. En otro orden de cosas, como el protocolo está basado en el sistema de cifrado de curva elíptica, se puede conseguir una mayor eficiencia de funcionamiento del protocolo, incluyendo menores intercambios de mensajes, menos ancho de banda de red ocupado, menor espacio de almacenamiento de la clave y una mayor velocidad de cálculo.

Las soluciones técnicas de los modos de realización descritos más arriba se pueden implementar mediante hardware y software, y el software se almacena en un medio de almacenamiento legible como, por ejemplo, un disco flexible, un disco duro o un disco óptico de un ordenador.

Las descripciones anteriores son únicamente modos de realización preferidos de la presente invención, pero no pretenden limitar la presente invención.

REIVINDICACIONES

1. Un método para generar una clave de grupo, en el que los parámetros del sistema se seleccionan basándose en una curva elíptica, comprendiendo el método:

formar (201), por parte de los miembros del grupo, una estructura con forma de estrella, y seleccionar un organizador entre los miembros del grupo;

seleccionar (203) individualmente de forma aleatoria, por parte de los miembros del grupo, valores DH secretos en función de los parámetros del sistema, generar individualmente valores DH públicos en función de los parámetros del sistema y los valores DH secretos seleccionados y difundir en el grupo los valores DH públicos;

seleccionar (204), por parte del organizador, un exponente secreto después de recibir los valores DH públicos de los otros miembros del grupo, calcular un valor DH del mensaje intermedio en función del exponente secreto, generar un mensaje intermedio que incluya el valor DH del mensaje intermedio, difundir en el grupo el mensaje intermedio, y generar una clave de grupo en función del valor DH secreto seleccionado por el organizador y de los valores DH públicos de los otros miembros del grupo; y

calcular (205), por parte de los otros miembros del grupo, después de recibir el mensaje intermedio, el valor DH secreto seleccionado por el organizador en función del mensaje intermedio y del valor DH público del organizador, verificar (206) que sea correcto el valor DH secreto calculado seleccionado por el organizador en función del valor DH público recibido del organizador, y generar (207) una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de los otros miembros del grupo.

2. El método de acuerdo con la reivindicación 1, en el que el cálculo (204) del valor DH del mensaje intermedio en función del exponente secreto comprende, además:

calcular el valor DH zP del mensaje intermedio en función del exponente secreto z, en donde el exponente secreto z es un número aleatorio seleccionado de un conjunto Z_q de restos no negativos mínimos obtenidos a partir de enteros módulo q, donde q es un número primo entre los parámetros del sistema y P es un punto base público en los parámetros del sistema.

3. El método de acuerdo con la reivindicación 2, en el que la generación (204) del mensaje intermedio que incluye el valor DH del mensaje intermedio comprende, además:

extraer una coordenada x, x, del valor DH del mensaje intermedio, zP, sobre la curva elíptica, y calcular un componente $r_1x \pmod p$ del mensaje intermedio del organizador en función del valor DH secreto r_1 seleccionado por el organizador, en donde p es un número primo entre los parámetros del sistema;

calcular los componentes $r_2zP, r_3zP, \ldots, r_nzP$ del mensaje intermedio de los otros miembros en función del exponente secreto z y de los valores DH públicos $X_i = r_iP$ difundidos por los otros miembros del grupo excepto el organizador, en donde $i = 2, \ldots, n$, y n es el número de miembros del grupo; y

generar el mensaje intermedio $\{c_1, c_2, \ldots, c_n\} = \{r_1x \pmod p, r_2zP, r_3zP, \ldots, r_nzP\}$ en función del componente del mensaje intermedio del organizador y los componentes del mensaje intermedio de los otros miembros; o

extraer una coordenada y, y, del valor DH del mensaje intermedio, zP, sobre la curva elíptica, y calcular un componente $r_1y \pmod p$ del mensaje intermedio del organizador en función del valor DH secreto r_1 seleccionado por el organizador, en donde p es un número primo entre los parámetros del sistema;

calcular los componentes $r_2zP, r_3zP, \ldots, r_nzP$ del mensaje intermedio de los otros miembros en función del exponente secreto z y de los valores DH públicos $X_i = r_iP$ difundidos por los otros miembros del grupo excepto el organizador, en donde $i = 2, \ldots, n$, y n es el número de miembros del grupo; y

generar el mensaje intermedio $\{c_1, c_2, \ldots, c_n\} = \{r_1y \pmod p, r_2zP, r_3zP, \ldots, r_nzP\}$ en función del componente del mensaje intermedio del organizador y los componentes del mensaje intermedio de los otros miembros.

4. El método de acuerdo con la reivindicación 3, en el que el cálculo del valor DH secreto seleccionado por el organizador en función del mensaje intermedio comprende, además:

calcular el valor DH del mensaje intermedio zP en función del mensaje intermedio $\{c_1, c_2, \ldots, c_n\} = \{r_1x \pmod p, r_2zP, r_3zP, \ldots, r_nzP\}$ y del valor DH secreto r_i, extraer la coordenada x, x, del valor DH del mensaje intermedio zP sobre la curva elíptica, y calcular el valor DH secreto $r_1 = c_1x^{-1} \pmod p$ seleccionado por el organizador; o

calcular el valor DH del mensaje intermedio zP en función del mensaje intermedio $\{c_1, c_2, \ldots, c_n\} = \{r_1y \pmod p, r_2zP, r_3zP, \ldots, r_nzP\}$ y del valor DH secreto r_i, extraer la coordenada y, y, del valor DH del mensaje intermedio zP

sobre la curva elíptica, y calcular el valor DH secreto $r_1 = c_1 y^{-1} (\text{mod } p)$ seleccionado por el organizador.

5. El método de acuerdo con la reivindicación 1, en el que la generación del clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de los otros miembros del grupo comprende, además:

generar la clave de grupo $K = r_1(r_2P + r_3P + \ldots + r_nP)$ en función de los valores DH públicos $X_i = r_iP$ de los otros miembros del grupo y el valor DH secreto r_1 seleccionado por el organizador, en donde $i = 2, \ldots, n$, n es el número de los miembros del grupo, y P es un punto base público en los parámetros del sistema.

6. El método de acuerdo con la reivindicación 1, en el que la verificación del valor DH secreto calculado seleccionado por el organizador en función del valor DH público recibido del organizador comprende, además:

calcular r_1P en función del valor DH secreto r_1 seleccionado por el organizador y el punto base público P seleccionado de los parámetros del sistema; y

verificar si el valor DH público X_1 recibido del organizador es o no igual al r_1P calculado, en donde si es igual el valor DH secreto es correcto.

7. El método de acuerdo con la reivindicación 1, en el que cuando se incorporan nuevos miembros al grupo, el método comprende, además:

formar, por parte de los nuevos miembros y los miembros del grupo, una nueva estructura con forma de estrella;

seleccionar individualmente de forma aleatoria, por parte del organizador y de los nuevos miembros, nuevos valores DH secretos en función de los parámetros del sistema, generar individualmente nuevos valores DH públicos en función de los parámetros del sistema y de los nuevos valores DH secretos, y difundir en el grupo los nuevos valores DH públicos;

tomar, por parte del organizador, una coordenada x o una coordenada y de la clave de grupo como un nuevo exponente secreto después de recibir los nuevos valores DH públicos, calcular un nuevo valor DH del mensaje intermedio en función del nuevo exponente secreto, generar un nuevo mensaje intermedio que incluye el nuevo valor DH del mensaje intermedio, difundir en el grupo el nuevo mensaje intermedio y generar una nueva clave de grupo en función del nuevo valor DH secreto seleccionado por el organizador y los nuevos valores DH públicos de los nuevos miembros; y

recibir, por parte de los otros miembros del grupo excepto el organizador, el nuevo mensaje intermedio del organizador, el nuevo valor DH público del organizador y los nuevos valores DH públicos de los nuevos miembros, calcular el nuevo valor DH secreto seleccionado por el organizador en función del nuevo mensaje intermedio, verificar que sea correcto el nuevo valor DH secreto calculado seleccionado por el organizador en función del nuevo valor DH público recibido del organizador, y generar una nueva clave de grupo en función del nuevo valor DH secreto seleccionado por el organizador y los nuevos valores DH públicos de los nuevos miembros del grupo.

8. El método de acuerdo con la reivindicación 7, en el que la generación del nuevo mensaje intermedio que incluye el nuevo valor DH del mensaje intermedio comprende, además:

extraer una coordenada x, *x',* del nuevo valor DH del mensaje intermedio, *z'P,* sobre la curva elíptica y calcular un componente $r_1' x' (\text{mod } p)$ del organizador del nuevo mensaje intermedio en función del nuevo valor DH secreto r_1' seleccionado por el organizador, en donde p es un número primo entre los parámetros del sistema, $z' = x_K$, x_K es una coordenada x de la clave de grupo, y P es un punto base público en los parámetros del sistema;

calcular los componentes de los nuevos miembros, $r_{n+1}' z' P, r_{n+2}' z' P, \ldots, r_{n+t}' z' P$, del nuevo mensaje intermedio en función del exponente secreto z' y de los valores DH públicos $X_i' = r_i' P$ difundidos por los nuevos miembros, en donde $i = n+1, \ldots, n+t$, n es el número de miembros del grupo antes de que los nuevos miembros se incorporen al grupo, y t es el número de nuevos miembros; y

generar el nuevo mensaje intermedio $\{c_1', c_{n+1}', \ldots, c_{n+t}'\} = \{r_1' x' (\text{mod } p), r_{n+1}' z' P, r_{n+2}' z' P, \ldots, r_{n+t}' z' P\}$ en función del componente del organizador del nuevo mensaje intermedio y de los componentes de los nuevos miembros del nuevo mensaje intermedio; o

extraer una coordenada y, *y',* del nuevo valor DH del mensaje intermedio, *z'P,* sobre la curva elíptica y calcular un componente $r_1' y' (\text{mod } p)$ del nuevo mensaje intermedio en función del nuevo valor DH secreto r_1' seleccionado por el organizador, en donde p es un número primo dentro de los parámetros del sistema, $z' = y_K$, y_K es una coordenada y de la clave de grupo, y P es un punto base público en los parámetros del sistema;

calcular los componentes de los nuevos miembros, $r_{n+1}' z' P, r_{n+2}' z' P, \ldots, r_{n+t}' z' P$, del nuevo mensaje intermedio

en función del exponente secreto *z'* y los valores DH públicos $X_i' = r_i' P$ difundidos por los nuevos miembros, en donde *i* = *n*+1, …, *n+t, n* es el número de miembros del grupo antes de que los nuevos miembros se incorporen al grupo, y *t* es el número de nuevos miembros; y

generar el nuevo mensaje intermedio $\{c_1', c_{n+1}', \ldots, c_{n+t}'\} = \{r_1' y' (\mathrm{mod}\ p), r_{n+1}' z' P, r_{n+2}' z' P, \ldots, r_{n+t}' z' P\}$ en función del componente del organizador del nuevo mensaje intermedio y de los componentes de los nuevos miembros del nuevo mensaje intermedio.

9. El método de acuerdo con la reivindicación 7, en el que la generación de la nueva clave de grupo en función del nuevo valor DH secreto seleccionado por el organizador y los nuevos valores DH públicos de los nuevos miembros comprende, además:

generar la clave de grupo $K' = r_1' (r_{n+1}' P, r_{n+2}' P, \ldots, r_{n+t}' P)$ en función de los valores DH públicos $X_i' = r_i' P$ de los nuevos miembros y del nuevo valor DH secreto r_1' seleccionado por el organizador, en donde *i* = *n*+1, …, *n+t, n* es el número de miembros del grupo antes de que los nuevos miembros se incorporen al grupo, *t* es el número de nuevos miembros, y *P* es el punto base público en los parámetros del sistema.

10. El método de acuerdo con la reivindicación 1, en el que cuando algunos miembros abandonan el grupo, el método comprende, además:

seleccionar (301), por parte del organizador, un nuevo valor DH secreto en función de los parámetros del sistema, generar un nuevo valor DH público en función de los parámetros del sistema y del nuevo valor DH secreto seleccionado, y difundir en el grupo el nuevo valor DH público;

seleccionar (302), por parte del organizador, un nuevo exponente secreto, calcular un nuevo valor DH del mensaje intermedio en función del nuevo exponente secreto, generar un nuevo mensaje intermedio que incluye el nuevo valor DH del mensaje intermedio, difundir en el grupo el nuevo mensaje intermedio, y generar una nueva clave de grupo en función del nuevo valor DH secreto seleccionado por el organizador y los valores DH públicos del resto de miembros del grupo excepto el organizador; y

calcular (306), por parte del resto de miembros del grupo excepto el organizador, el nuevo valor DH secreto seleccionado por el organizador en función del nuevo mensaje intermedio después de recibir el nuevo mensaje intermedio y del nuevo valor DH público del organizador, verificar que sea correcto el nuevo valor DH secreto en función del nuevo valor DH público del organizador recibido, y generar una nueva clave de grupo en función del nuevo valor DH secreto y de los valores DH públicos del resto de miembros del grupo excepto el organizador.

11. El método de acuerdo con la reivindicación 10, en el que la generación del nuevo mensaje intermedio que incluye el nuevo valor DH del mensaje intermedio comprende, además:

extraer una coordenada x, *x',* del nuevo valor DH del mensaje intermedio, *z'P,* sobre la curva elíptica, y calcular un componente del organizador, $r_1' x' (\mathrm{mod}\ p)$, del nuevo mensaje intermedio en función del nuevo valor DH secreto r_1' seleccionado por el organizador, en donde *p* es un número primo entre los parámetros del sistema;

calcular los componentes del resto de miembros, $r_2' z' P, \ldots, r_{j_1-1}' z' P, r_{j_1+1}' z' P, \ldots, r_{j_k-1}' z' P, r_{j_k+1}' z' P, \ldots, r_n' z' P$, del nuevo mensaje intermedio en función del exponente secreto *z'* y de los valores DH públicos $X_i' = r_i' P$ difundidos por el resto de miembros del grupo excepto el organizador, en donde *i* = 2, …, j_1-1, j_1+1,…, j_k-1, j_k+1, …, *n*, y *k* es el número de los miembros que abandonan el grupo; y

generar el nuevo mensaje intermedio $\{c_1', \ldots, c''_{j_1-1}, c'_{j_1+1}, \ldots, c'_{j_k-1}, c'_{j_k+1}, \ldots, c'_n\} = \{r_1' x' (\mathrm{mod}\ p), \ldots, r_{j_1-1}' z' P, r_{j_1+1}' z' P, \ldots, r_{j_k-1}' z' P, r_{j_k+1}' z' P, \ldots, r_n' z' P\}$ en función del componente del organizador del nuevo mensaje intermedio y los componentes del resto de miembros del nuevo mensaje intermedio; o

extraer una coordenada y, *y',* del nuevo valor DH del mensaje intermedio, *z'P,* sobre la curva elíptica, y calcular un componente del organizador, $r_1' y' (\mathrm{mod}\ p)$, del nuevo mensaje intermedio en función del nuevo valor DH secreto r_1' seleccionado por el organizador, en donde *p* es un número primo entre los parámetros del sistema;

calcular los componentes del resto de miembros, $r_2' z' P, \ldots, r_{j_1-1}' z' P, r_{j_1+1}' z' P, \ldots, r_{j_k-1}' z' P, r_{j_k+1}' z' P, \ldots, r_n' z' P$, del nuevo mensaje intermedio en función del exponente secreto *z'* y de los valores DH públicos $X_i' = r_i' P$ difundidos por el resto de miembros del grupo excepto el organizador, en donde *i* = 2, …, j_1-1, j_1+1,…, j_k-1, j_k+1, …, *n*, y *k* es el número de los miembros que abandonan el grupo; y

generar el nuevo mensaje intermedio $\{c_1', \ldots, c''_{j_1-1}, c'_{j_1+1}, \ldots, c'_{j_k-1}, c'_{j_k+1}, \ldots, c'_n\} = \{r_1' y' (\mathrm{mod}\ p), \ldots, r_{j_1-1}' z' P, r_{j_1+1}' z' P, \ldots, r_{j_k-1}' z' P, r_{j_k+1}' z' P, \ldots, r_n' z' P\}$ en función del componente del organizador del nuevo mensaje intermedio y de los componentes del resto de miembros

del nuevo mensaje intermedio.

12. Un sistema para generar una clave de grupo, que comprende: un dispositivo de comunicación que actúa como organizador y unos dispositivos de comunicación que actúan como miembros;

en donde el dispositivo de comunicación que actúa como organizador está configurado para seleccionar un valor DH secreto en función de los parámetros del sistema, generar un valor DH público en función de los parámetros del sistema y del valor DH secreto seleccionado, y difundir en el grupo el valor DH público; y después de recibir los valores DH públicos de otros dispositivos, el dispositivo de comunicación que actúa como organizador está configurado, además, para seleccionar un exponente secreto, calcular un valor DH del mensaje intermedio en función del exponente secreto, generar un mensaje intermedio que incluye el valor DH del mensaje intermedio, difundir en el grupo el mensaje intermedio, y generar una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de todos los dispositivos del grupo; y

los dispositivos de comunicación que actúan como miembros están configurados para seleccionar los valores DH secretos en función de los parámetros del sistema, generar valores DH públicos en función de los parámetros del sistema y de los valores DH secretos seleccionados, y difundir los valores DH públicos; y después de recibir el valor DH público y el mensaje intermedio difundidos por el dispositivo de comunicación que actúa como organizador, los dispositivos de comunicación que actúan como miembros están configurados, además, para calcular el valor DH secreto seleccionado por el organizador en función del mensaje intermedio, verificar que sea correcto el valor DH secreto calculado seleccionado por el organizador, y generar una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de todos los dispositivos del grupo.

13. Un dispositivo de comunicación, que comprende:

un módulo de selección de parámetros del sistema, configurado para seleccionar parámetros del sistema a partir de una curva elíptica;

un módulo de generación y difusión del valor DH público, configurado para seleccionar un valor DH secreto en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, generar un valor DH público en función de los parámetros del sistema y del valor DH secreto seleccionado, y difundir el valor DH público;

un módulo de generación y difusión del mensaje intermedio, configurado para seleccionar un exponente secreto después de recibir los valores DH públicos difundidos por otros dispositivos de comunicación, calcular un valor DH del mensaje intermedio en función del exponente secreto, generar un mensaje intermedio que incluye el valor DH del mensaje intermedio en función del valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público, y difundir el mensaje intermedio; y

un módulo de generación de la clave de grupo del organizador, configurado para recibir los valores DH públicos difundidos por otros dispositivos de comunicación, y generar una clave de grupo en función del valor DH secreto seleccionado por el módulo de generación y difusión del valor DH público y los valores DH públicos difundidos por otros dispositivos de comunicación.

14. Un dispositivo de comunicación, que comprende:

un módulo de selección de parámetros del sistema, configurado para seleccionar parámetros del sistema a partir de una curva elíptica;

un módulo de generación y difusión del valor DH público, configurado para seleccionar valores DH secretos en función de los parámetros del sistema seleccionados por el módulo de selección de parámetros del sistema, generar valores DH públicos en función de los parámetros del sistema y de los valores DH secretos seleccionados, y difundir los valores DH públicos; y

un módulo de generación de la clave de grupo del miembro, configurado para recibir un valor DH público y un mensaje intermedio difundido por otro dispositivo de comunicación, calcular un valor DH secreto seleccionado por un organizador en función del mensaje intermedio, verificar que sea correcto el valor DH secreto calculado seleccionado por el organizador en función del valor DH público difundido por el dispositivo de comunicación que difunde el mensaje intermedio, y a continuación generar una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos difundidos por los otros dispositivos de comunicación excepto el dispositivo de comunicación que difunde el mensaje intermedio.

15. El dispositivo de comunicación de acuerdo con la reivindicación 13 ó 14, que comprende, además:

un módulo de actualización de la clave de grupo, configurado para ordenar al módulo de generación y difusión del valor DH público que genere y difunda nuevos valores DH públicos para los nuevos miembros cuando se incorporen nuevos miembros al grupo.

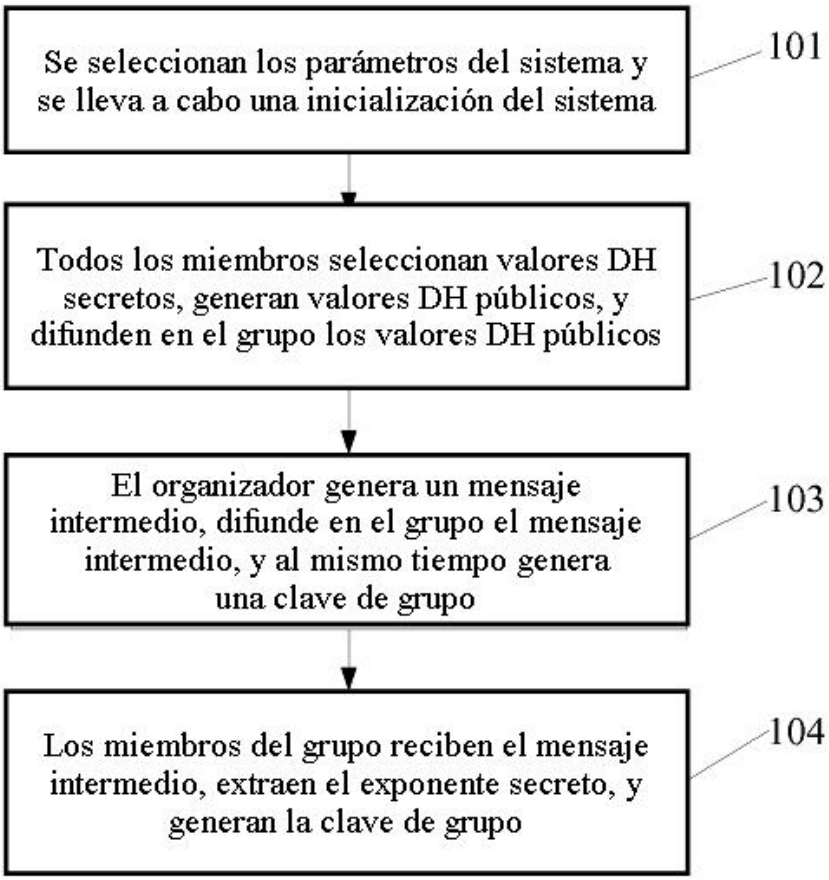
Se seleccionan los parámetros del sistema y se lleva a cabo una inicialización del sistema
101
Todos los miembros seleccionan valores DH secretos, generan valores DH públicos, y difunden en el grupo los valores DH públicos
102
El organizador genera un mensaje intermedio, difunde en el grupo el mensaje intermedio, y al mismo tiempo genera una clave de grupo
103
Los miembros del grupo reciben el mensaje intermedio, extraen el exponente secreto, y generan la clave de grupo
104

FIG. 1

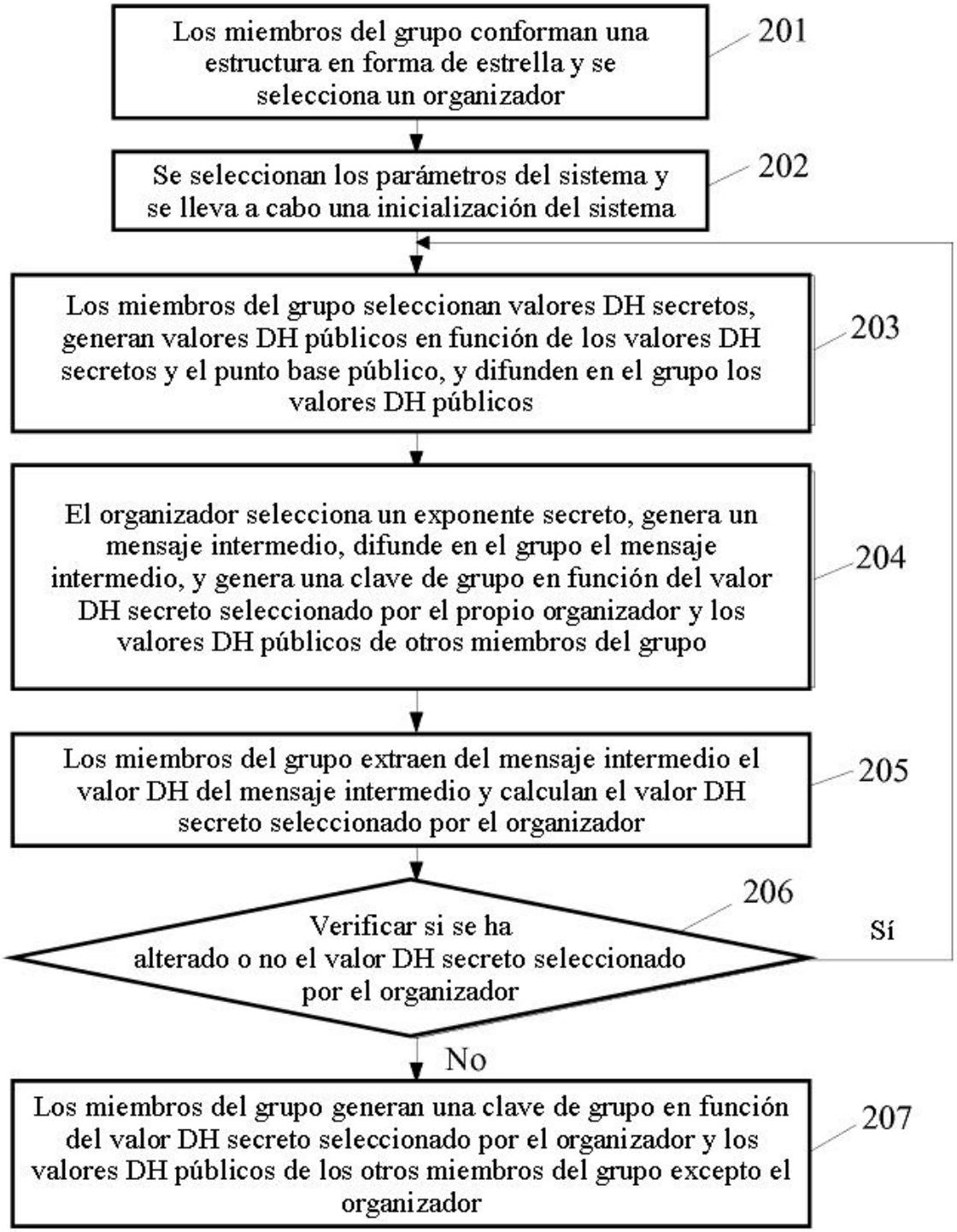
Los miembros del grupo conforman una estructura en forma de estrella y se selecciona un organizador
201
Se seleccionan los parámetros del sistema y se lleva a cabo una inicialización del sistema
202
Los miembros del grupo seleccionan valores DH secretos, generan valores DH públicos en función de los valores DH secretos y el punto base público, y difunden en el grupo los valores DH públicos
203
El organizador selecciona un exponente secreto, genera un mensaje intermedio, difunde en el grupo el mensaje intermedio, y genera una clave de grupo en función del valor DH secreto seleccionado por el propio organizador y los valores DH públicos de otros miembros del grupo
204
Los miembros del grupo extraen del mensaje intermedio el valor DH del mensaje intermedio y calculan el valor DH secreto seleccionado por el organizador
205
Verificar si se ha alterado o no el valor DH secreto seleccionado por el organizador
206
Sí
No
Los miembros del grupo generan una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de los otros miembros del grupo excepto el organizador
207

FIG. 2

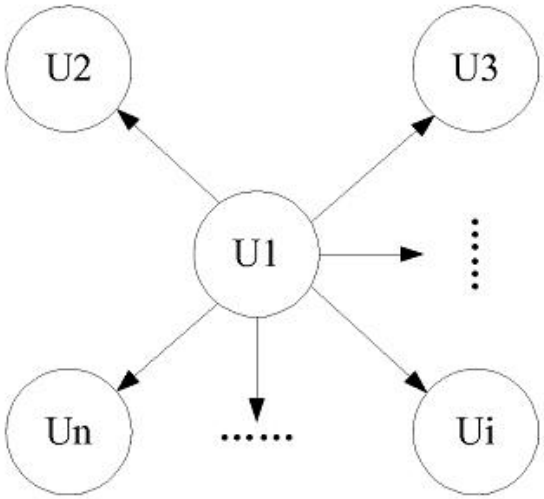

FIG. 3

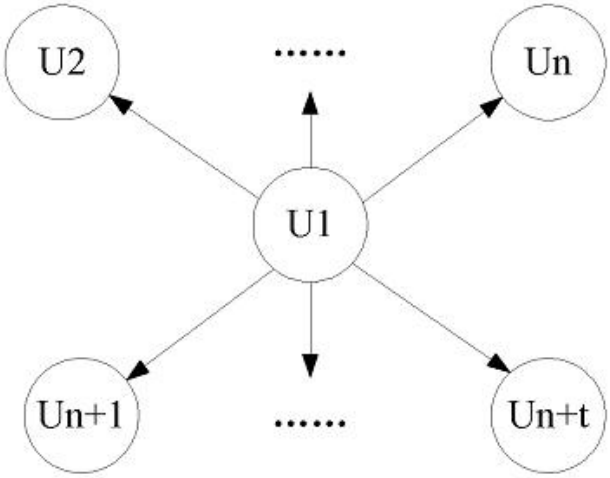

FIG. 4

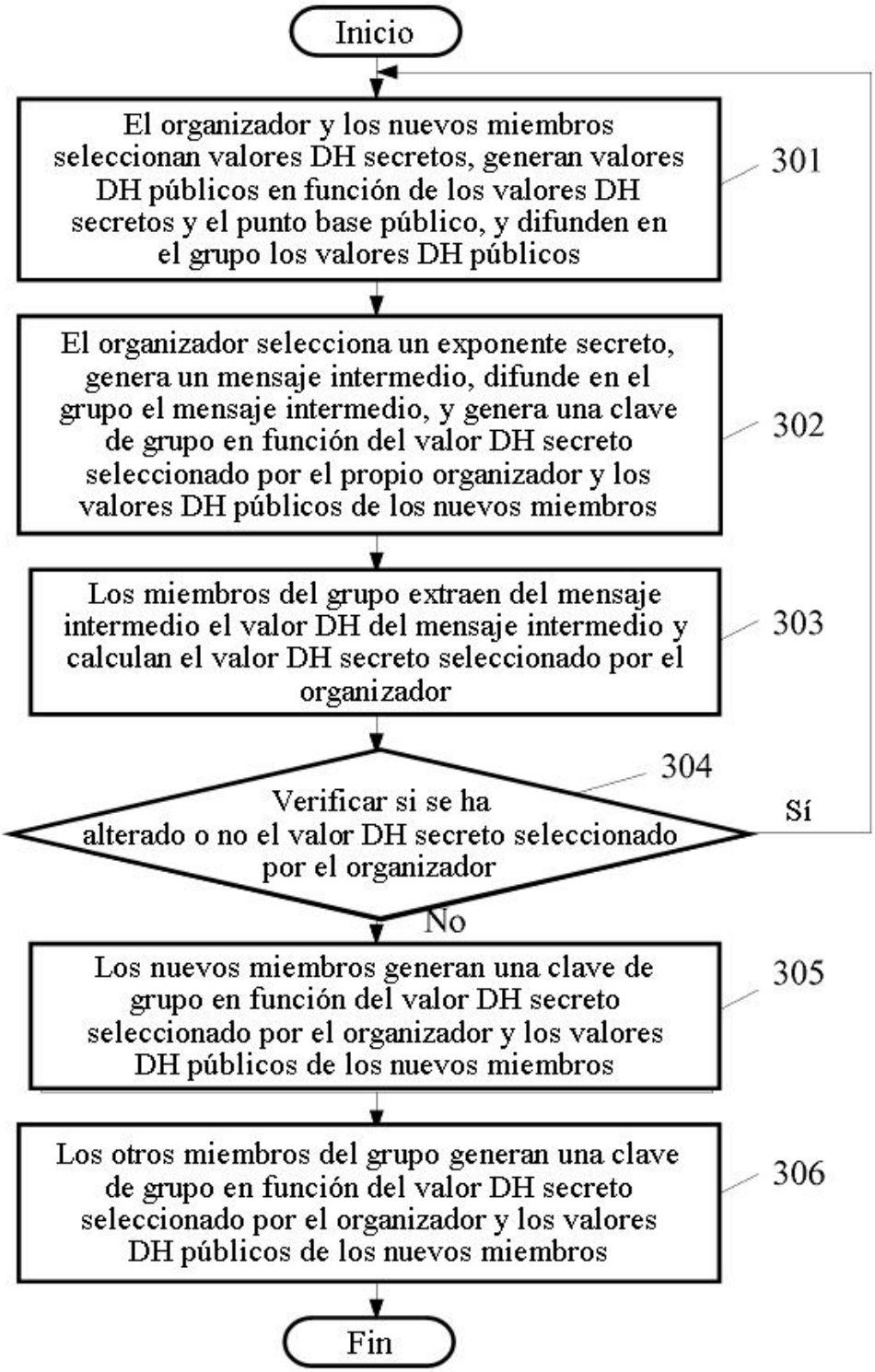
Inicio
El organizador y los nuevos miembros seleccionan valores DH secretos, generan valores DH públicos en función de los valores DH secretos y el punto base público, y difunden en el grupo los valores DH públicos
301
El organizador selecciona un exponente secreto, genera un mensaje intermedio, difunde en el grupo el mensaje intermedio, y genera una clave de grupo en función del valor DH secreto seleccionado por el propio organizador y los valores DH públicos de los nuevos miembros
302
Los miembros del grupo extraen del mensaje intermedio el valor DH del mensaje intermedio y calculan el valor DH secreto seleccionado por el organizador
303
304
Verificar si se ha alterado o no el valor DH secreto seleccionado por el organizador
Sí
No
Los nuevos miembros generan una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de los nuevos miembros
305
Los otros miembros del grupo generan una clave de grupo en función del valor DH secreto seleccionado por el organizador y los valores DH públicos de los nuevos miembros
306
Fin

FIG. 5

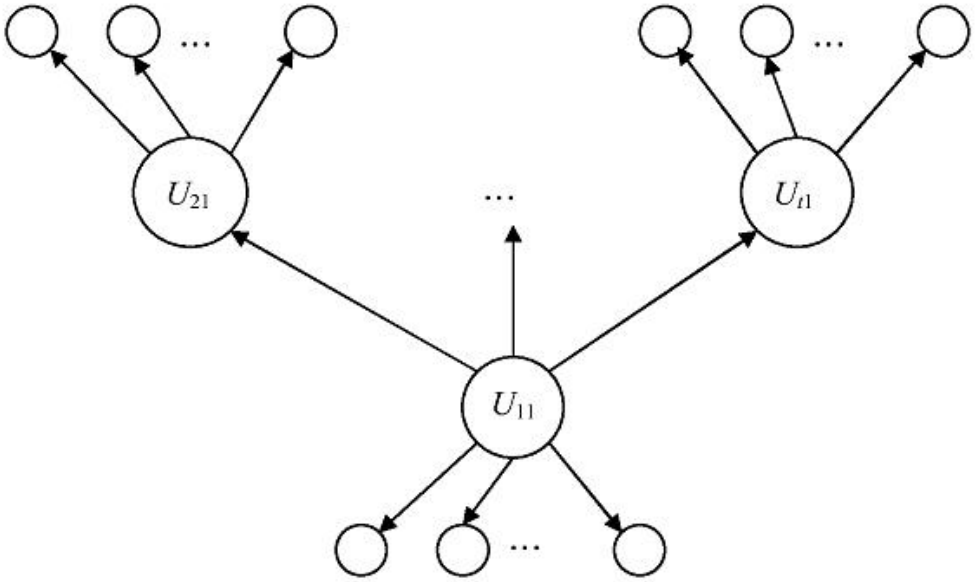

FIG. 6

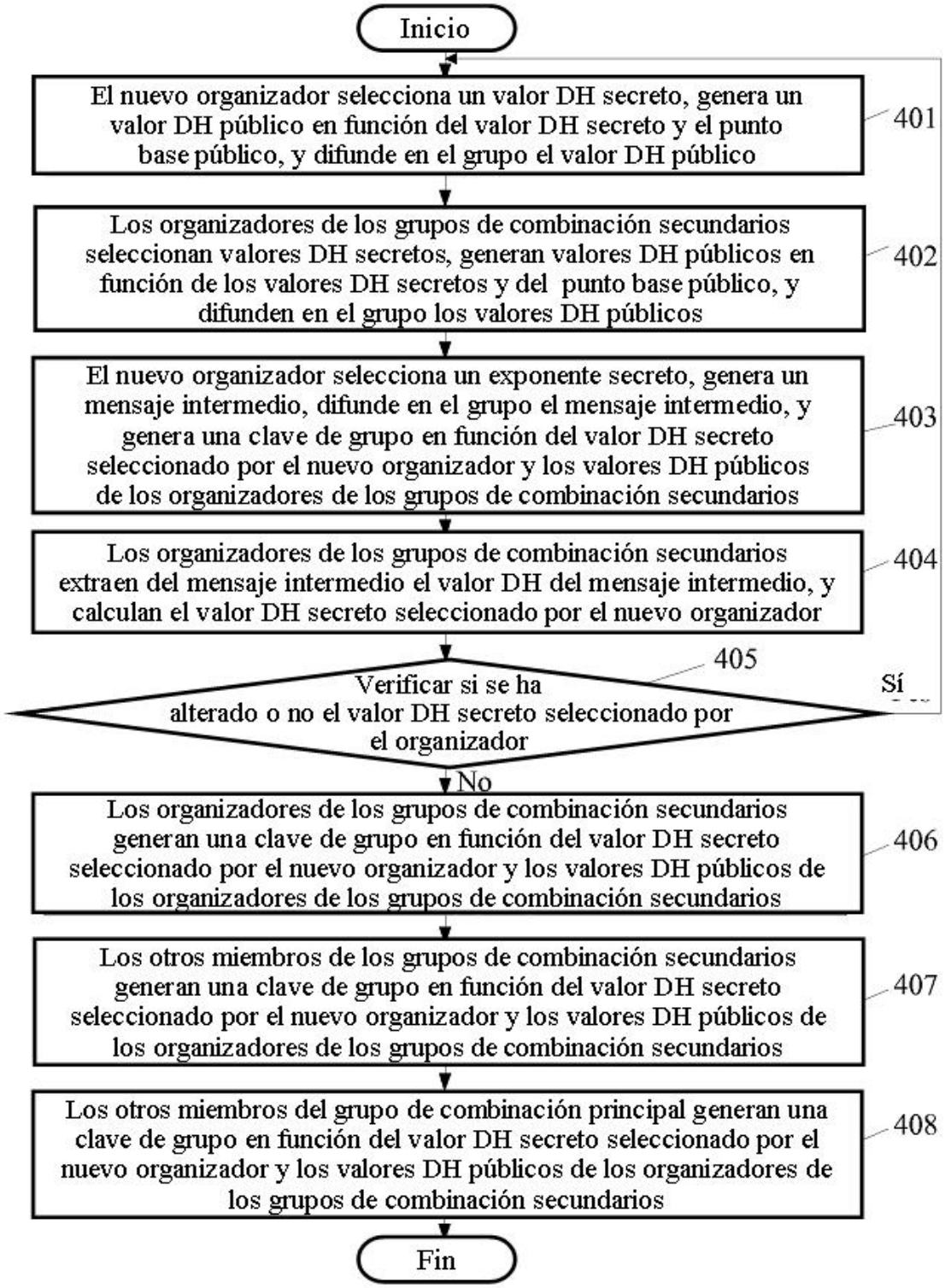
Inicio
El nuevo organizador selecciona un valor DH secreto, genera un valor DH público en función del valor DH secreto y el punto base público, y difunde en el grupo el valor DH público
401
Los organizadores de los grupos de combinación secundarios seleccionan valores DH secretos, generan valores DH públicos en función de los valores DH secretos y del punto base público, y difunden en el grupo los valores DH públicos
402
El nuevo organizador selecciona un exponente secreto, genera un mensaje intermedio, difunde en el grupo el mensaje intermedio, y genera una clave de grupo en función del valor DH secreto seleccionado por el nuevo organizador y los valores DH públicos de los organizadores de los grupos de combinación secundarios
403
Los organizadores de los grupos de combinación secundarios extraen del mensaje intermedio el valor DH del mensaje intermedio, y calculan el valor DH secreto seleccionado por el nuevo organizador
404
405
Verificar si se ha alterado o no el valor DH secreto seleccionado por el organizador
Sí
No
Los organizadores de los grupos de combinación secundarios generan una clave de grupo en función del valor DH secreto seleccionado por el nuevo organizador y los valores DH públicos de los organizadores de los grupos de combinación secundarios
406
Los otros miembros de los grupos de combinación secundarios generan una clave de grupo en función del valor DH secreto seleccionado por el nuevo organizador y los valores DH públicos de los organizadores de los grupos de combinación secundarios
407
Los otros miembros del grupo de combinación principal generan una clave de grupo en función del valor DH secreto seleccionado por el nuevo organizador y los valores DH públicos de los organizadores de los grupos de combinación secundarios
408
Fin

FIG. 7

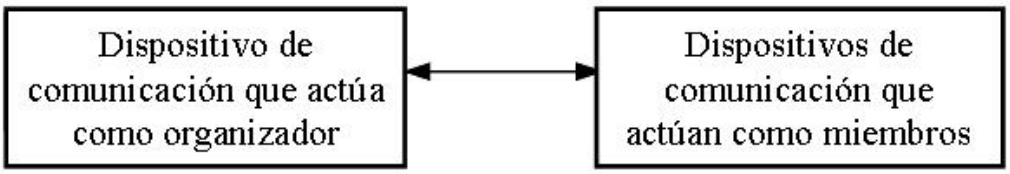
Dispositivo de comunicación que actúa como organizador
Dispositivos de comunicación que actúan como miembros

FIG. 8

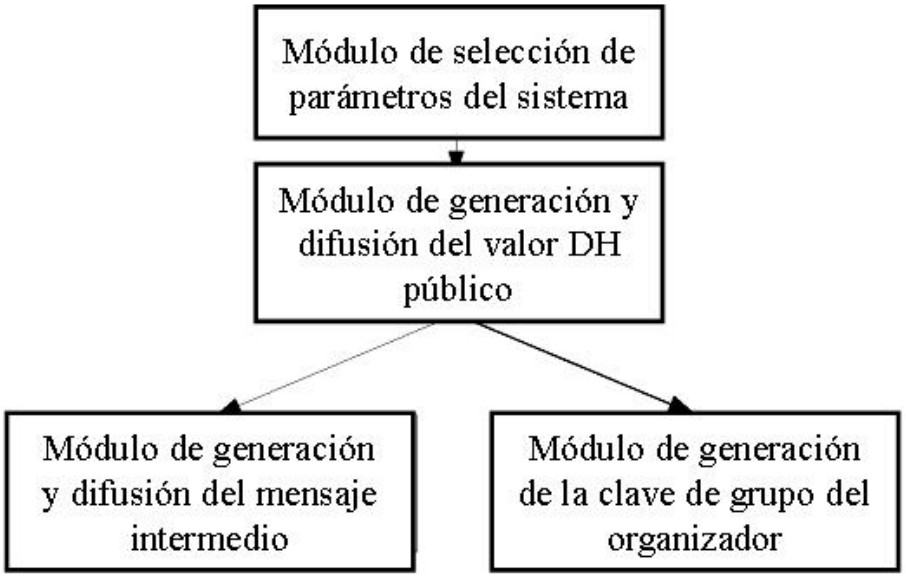
Módulo de selección de parámetros del sistema
Módulo de generación y difusión del valor DH público
Módulo de generación y difusión del mensaje intermedio
Módulo de generación de la clave de grupo del organizador

FIG. 9

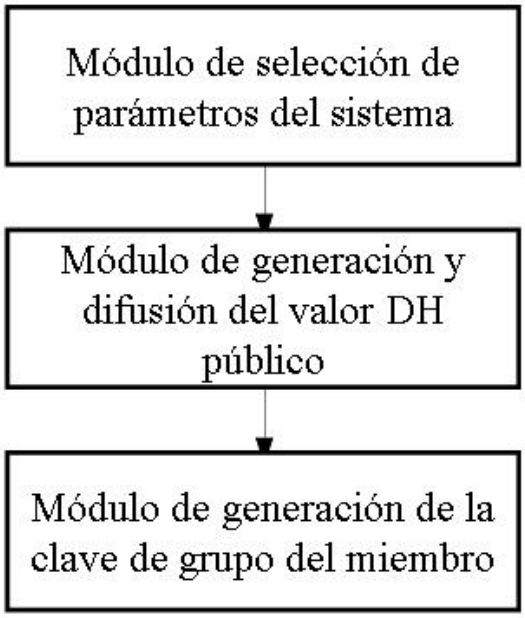
Módulo de selección de parámetros del sistema
Módulo de generación y difusión del valor DH público
Módulo de generación de la clave de grupo del miembro

FIG. 10