(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 448 806**

(51) Int. CI.:

H04L 9/06 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.01.2011 E 11704404 (0)**

(97) Fecha y número de publicación de la concesión europea: **11.12.2013 EP 2540027**

(54) Título: **Red de distribución inteligente y procedimiento para operar una red de distribución inteligente**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.03.2014

(73) Titular/es:

NEC EUROPE LTD. (50.0%)
Kurfürsten-Anlage 36
69115 Heidelberg, DE y
UNIVERSIDAD DE MURCIA (50.0%)

(72) Inventor/es:

GÓMEZ MÁRMOL, FÉLIX;
SORGE, CHRISTOPH;
UGUS, OSMAN;
MARTÍNEZ PÉREZ, GREGORIO y
HESSLER, ALBAN

(74) Agente/Representante:

ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Red de distribución inteligente y procedimiento para operar una red de distribución inteligente.

La presente invención se refiere a una red de distribución inteligente y un procedimiento para operar una red de distribución inteligente que incluye una pluralidad de medidores inteligentes, estando configurados dichos medidores inteligentes para monitorizar al menos una cantidad física medida y para proporcionar resultados de medición de dicha al menos una cantidad física medida a una entidad central.

Las redes de distribución del tipo descrito inicialmente están adquiriendo cada vez más importancia. En particular, en el campo de la distribución de energía eléctrica, las redes de distribución eléctrica globales están a punto de la mayor transformación tecnológica desde la introducción de la electricidad en el hogar. La infraestructura anticuada que distribuye energía a nuestros hogares y negocios está siendo sustituida por una colección de sistemas digitales denominada la red de distribución inteligente. Esta red de distribución es la modernización del sistema eléctrico existente que mejora la capacidad de los clientes y las empresas de servicio público de monitorizar, controlar, y predecir el uso de energía.

El dispositivo de monitorización y notificación de utilización en el emplazamiento de cada cliente se denomina el *medidor inteligente*, que es una clase de contador “inteligente”. El medidor inteligente es un sustituto informatizado del medidor eléctrico acoplado al exterior de muchos de nuestros hogares hoy en día. Típicamente, un medidor inteligente contiene un procesador, almacenamiento no volátil, e instalaciones de comunicación. Aunque en muchos sentidos, la apariencia y función del medidor inteligente es igual que su predecesor poco sofisticado, sus características adicionales lo hacen más útil. Las características adicionales incluyen, en particular, seguimiento de la utilización como una función de la hora del día, desconexión de un cliente mediante software, o envío de alarmas en caso de problemas.

Los medidores inteligentes pueden proporcionar mediciones de consumo de energía a los suministradores de energía (casi) instantáneamente. Esto es bastante beneficioso para la red de distribución inteligente porque permite una mejora en la capacidad de monitorizar, controlar y predecir el uso de energía, entre otras ventajas. Sin embargo, pueden presentarse algunas cuestiones de privacidad, ya que tal monitorización podría revelar la presencia de usuarios finales en sus casas, qué aparatos eléctricos están usando en cada momento, o incluso sus hábitos diarios en el hogar, tal como se muestra en la Fig. 1. Por lo tanto, el riesgo del despliegue de una red de distribución inteligente radica en el peligro de que los clientes se vuelvan clientes “transparentes”, ya que la monitorización y el análisis (potencialmente malicioso) de datos de consumo individual contempla conclusiones de gran alcance acerca de los estilos de vida de los clientes.

Cabe destacar que aunque la presente descripción está relacionada sobre todo con medidores inteligentes para monitorizar el consumo de energía eléctrica, también es posible medir en una casa el consumo de agua, gas, calor o similares.

El artículo de Claude Castelluccia y col.: “Efficient and provably secure aggregation of encrypted data in wireless sensor networks”, ACM Transactions on Sensor Networks, vol. 5, nº 3, 1 de mayo de 2009, describe un procedimiento de agregación de datos en una red de sensores inalámbricos para monitorizar cantidades físicas. Los sensores están dispuestos en un árbol jerárquico que se extiende desde una entidad central designada como sumidero. Cada sensor cifra su valor medido por el mismo esquema de cifrado (bi)homomórfico y lo envía hacia el sumidero. Sensores intermedios en el árbol agregan los datos sumando los valores cifrados. Debido a la propiedad de homomorfismo, la suma de los valores cifrados puede descifrarse en la suma de los valores de texto sin cifrar usando la suma de las claves de los sensores. Las claves individuales de los sensores se generan a partir de un secreto de grupo y los ID de sensores únicos.

Por lo tanto, un objeto de la presente invención es mejorar y desarrollar más a fondo una red de distribución inteligente y un procedimiento para operar una red de distribución inteligente del tipo descrito inicialmente de tal modo que, empleando mecanismos que sean fáciles de implementar, las cuestiones de privacidad de los usuarios finales/clientes se preserven de un modo fiable y eficiente.

De acuerdo con la invención, el objeto anteriormente mencionado se logra mediante un procedimiento que comprende las características de la reivindicación 1. Según esta reivindicación, tal procedimiento está caracterizado en las siguientes etapas:

dicha red de distribución inteligente es dividida en grupos G de medidores inteligentes sm_i, de manera que cada uno de dichos medidores inteligentes pertenece exactamente a un grupo,

todos los medidores inteligentes sm_i de uno de dichos grupos cifran su valor medido e_i aplicando un esquema de cifrado bihomomórfico E_{ki} y lo envían a dicha entidad central ES,

un medidor inteligente por grupo es designado como agregador de claves al que todos los medidores inteligentes sm_i de ese grupo envían su clave k_i empleada para dicho cifrado,

dicho agregador de claves calcula la agregación de todas las claves recibidas k_i y envía la clave agregada K a dicha entidad central ES,

dicha entidad central ES agrega todos los valores medidos cifrados recibidos e_i y descifra dicha agregación empleando dicha clave agregada K.

Además, el objeto anteriormente mencionado se logra mediante una red de distribución inteligente que comprende las características de la reivindicación 21. Según esta reivindicación, tal red de distribución inteligente está caracterizada porque dicha red de distribución inteligente está dividida en grupos G de medidores inteligentes sm_i, de manera que cada uno de dichos medidores inteligentes pertenece exactamente a un grupo,

en la que todos los medidores inteligentes sm_i de uno de dichos grupos están configurados para cifrar su valor medido e_i aplicando un esquema de cifrado bihomomórfico E_{ki} y enviarlo a dicha entidad central ES,

en la que un medidor inteligente por grupo es designado como agregador de claves al que todos los medidores inteligentes sm_i de ese grupo envían su clave k_i empleada para dicho cifrado,

en la que dicho agregador de claves incluye medios para calcular la agregación de todas las claves recibidas k_i y para enviar la clave agregada K a dicha entidad central ES,

en la que dicha entidad central ES está configurada para agregar todos los valores medidos cifrados recibidos e_i y para descifrar dicha agregación empleando dicha clave agregada K.

Según la invención, se ha reconocido que el cifrado/decifrado bihomomórfico de las mediciones de variables físicas de medición, en particular el consumo de energía, puede emplearse para garantizar la integridad y la confidencialidad de los valores de medición. En la medida de lo posible, la presente invención proporciona una arquitectura de privacidad mejorada para medición inteligente para conseguir la protección de la privacidad de los usuarios finales, por ejemplo, con respecto a sus hábitos de consumo de energía. La presente invención impide que la entidad central averigüe las mediciones de los medidores inteligentes individuales, pero le permite conocer la agregación de los mismos.

En otras palabras, a la entidad central se le proporciona una agregación de valores cifrados (los informes de los medidores inteligentes individuales). La entidad central no puede descifrar tales valores individuales (preservando de este modo la privacidad del los usuarios), pero sí que puede descifrar la agregación de los mismos, por medio de un cifrado bihomomórfico. Un esquema de cifrado bihomomórfico es un esquema de cifrado simétrico que es homomórfico tanto en el espacio de texto sin cifrar como en el espacio de claves. De este modo, aunque se preserva la privacidad de los usuarios individuales, la entidad central, por ejemplo, un suministrador de electricidad, puede monitorizar con exactitud la cantidad de energía (o agua, gas, calor, etc., según el caso) necesitada por sus clientes. Aunque esto no es necesario para la operación técnica de la red de distribución de electricidad, la información puede usarse para comerciar con energía eléctrica. Incluso hoy en día, cada suministrador de electricidad tiene que comprar la cantidad de energía usada por sus clientes en cualquier momento específico. Sin embargo, esto está basado actualmente en una estimación (usando el consumo global de electricidad de esos clientes a lo largo de un año entero y suponiendo ciertas curvas de carga basadas en la experiencia previa). Además, la información actualizada agregada acerca de la utilización de energía de ciertos grupos puede mejorar las previsiones acerca de la carga de la red de distribución de electricidad en el futuro inmediato. Esta información es útil para planificar, por ejemplo, qué plantas eléctricas usar.

De acuerdo con la invención, la agrupación de medidores inteligentes desvincula entre sí al remitente de un informe y a tal informe, preservando así su privacidad respecto a la entidad central. Además, el despliegue de un agregador de claves de una manera tal como la descrita anteriormente tiene como resultado que, i) nadie conoce las claves de otros miembros (excepto el agregador de claves), y ii) no importa si el agregador actúa maliciosamente y comparte las claves recibidas con la entidad central porque ésta no puede vincular o relacionar cada clave con cada valor de medición recibido desde ese grupo.

Según una realización preferida, puede estar previsto que la al menos una cantidad física medida específica sea el consumo de energía eléctrica de una unidad consumidora, en particular una casa, una empresa, una planta, o similar. En tal caso, la entidad central puede ser un suministrador de energía. En este contexto es importante observar que el suministrador de electricidad no es necesariamente idéntico al proveedor de la red de distribución eléctrica (aunque, en algunos casos, realmente lo es).

Con respecto a una disposición estructurada y natural de los grupos de medidores inteligentes, puede estar previsto que grupos de medidores inteligentes sean configurados metiendo en el mismo grupo, por ejemplo, todos los

medidores inteligentes que pertenecen a un edificio específico, calle, barrio, pueblo o similar. En cualquier caso, cabe destacar que todos los medidores inteligentes dentro del mismo grupo también pertenecen al mismo suministrador de energía. Por ejemplo, el grupo G_k estaría compuesto por

$$G_k = \{sm_1^k, sm_2^k, ..., sm_n^k\}.$$

Con respecto a mantener la entidad central fiablemente actualizada, puede estar previsto que los medidores inteligentes notifique sus mediciones a la entidad central en intervalos de tiempo regulares, que pueden considerarse como periodos de notificación.

Ventajosamente, para asegurar la transmisión segura de datos puede estar previsto que los medidores inteligentes notifiquen sus mediciones a la entidad central a través de un canal seguro. El establecimiento de un canal seguro requiere el uso de un mecanismo de autenticación. En teoría, podría usarse cualquier mecanismo de autenticación; los más adecuados, para autenticar el medidor inteligente sólo como un miembro de un grupo de medidores inteligentes autorizados, serían firmas de grupo o esquemas de credenciales anónimas. Como consecuencia, se asegura que el agregador de claves no pueda descifrar los valores enviados por cada medidor inteligente, aunque conozca sus claves, ya que los anteriores se envían a la entidad central a través de un canal seguro.

Con respecto a la mejora adicional de la seguridad, puede estar previsto que un medidor inteligente por grupo sea designado sólo periódicamente como el agregador de claves, es decir, que el medidor inteligente que es designado como agregador de claves dentro del grupo se cambia de vez en cuando. En particular, puede estar previsto que se realice un cambio del agregador de claves en caso de que un medidor inteligente que esté designado como agregador de claves falle, abandone el grupo y/o se descubra que actúa maliciosamente. En cualquier caso, puede estar previsto que el resto de medidores inteligentes miembros de un grupo envíen sus claves al agregador de claves de un modo seguro.

Una vez que el agregador de claves ha recibido todas las claves de los miembros del grupo, las agrega para obtener la clave agregada *K* del siguiente modo:

$$K = f(k_1, k_2, ..., k_n) = \oplus_{i=1}^{n} k_i = \sum_{i=1}^{n} k_i .$$

Luego, envía la clave agregada *K* a la entidad central a través de un canal seguro. Para mantener la tara de señalización lo más baja posible, puede estar previsto que la clave agregada *K* sea enviada a la entidad central sólo una vez la primera vez, es decir, en conexión con un primer periodo de informes de medición de un grupo de medidores inteligentes. Posteriormente, la clave agregada *K* tiene que ser enviada a la entidad central sólo cada vez que un medidor inteligente falla y/o abandona o entra/se une al grupo respectivo.

Según una realización preferida se definen periodos de notificación, en los que cada medidor inteligente de un grupo usa una clave diferente por periodo de notificación para cifrar su valor de medición de ese periodo. Cambiando la clave de un medidor inteligente cada periodo de notificación se mejora más la seguridad del proceso ya que se hace casi imposible que un participante malicioso descifre los valores medidos. Ventajosamente, para permitir el descifrado sin esfuerzo por parte de la entidad central, las claves que se emplean para cada periodo de notificación pueden calcularse de tal modo que la agregación de todas las claves de todos los medidores inteligentes de un grupo siempre permanezca igual, es decir, la clave agregada *K* permanece constante. Como consecuencia, como ya se resumió anteriormente, el número de mensajes de notificación de la clave agregada *K* desde el agregador de claves a la entidad central puede minimizarse.

En una realización específica puede estar previsto que los medidores inteligentes dentro del mismo grupo formen un "anillo", en el que cada medidor inteligente envía al siguiente en el anillo un valor aleatorio δ_i a través de un canal seguro, el cual se resta de su clave y se suma a la clave del siguiente medidor inteligente de la siguiente manera:

$$k_{i,j} = k_{i,j-1} - \delta_{i,j} + \delta_{i-1,j} .$$

En otras palabras, cada medidor inteligente sm_i, para establecer una nueva clave $k_{i,j}$ para un periodo de notificación subsiguiente *j*, resta de su clave $k_{i,j-1}$ empleada en el periodo de notificación precedente *j-1* el valor aleatorio $\delta_{i,j}$ enviado al siguiente medidor inteligente dentro del anillo y suma el valor aleatorio $\delta_{i-1,j}$ recibido desde el medidor inteligente precedente dentro del anillo.

Si un medidor inteligente dentro de un grupo falla, o actúa defectuosa o incluso maliciosamente, e intenta subvertir el sistema enviando su clave al agregador de claves, pero no el valor de medición cifrado correspondiente (o

viceversa), entonces la entidad central no puede realizar el descifrado correcto.

Para abordar esta cuestión e impedir los medidores inteligentes maliciosos/defectuosos, según una realización preferida puede aplicarse un mecanismo adicional, denominado en lo sucesivo “solución de testigos”. Esta “solución de testigos” puede realizarse de la siguiente manera:

a) Cada medidor inteligente sm_i envía su clave k_{ij} al agregador de claves *KA* a través de un canal seguro

b) El agregador de claves *KA*, en el momento de recibir una clave procedente de un medidor inteligente, responde con un testigo de acuse de recibo (denominado en lo sucesivo testigo ACK), $T_{KA,i}$

c) Cada medidor inteligente sm_i envía entonces la medición cifrada $E_{ki,j}$ (e_{ij}), junto con el testigo ACK $T_{KA,i}$, a la entidad central

d) La entidad central sólo acepta mediciones cifradas procedentes de medidores inteligentes que vienen con tales testigos

e) La entidad central responde con otro testigo ACK, $T_{CE,i}$, directamente al agregador de claves *KA*

f) Una vez que el agregador de claves recibe tal testigo $T_{CE,i}$, acepta realmente la clave k_{ij} recibida en la etapa a)

La etapa d) asegura que sea imposible enviar un valor cifrado sin haber enviado previamente la clave al agregador de claves. A su vez, la etapa e) excluye la posibilidad de que un medidor inteligente pudiera enviar su clave al agregador de claves, sin enviar la medición cifrada a la entidad central.

De nuevo, para mantener la tara de señalización lo más baja posible la solución de testigos resumida anteriormente puede habilitarse sólo durante un periodo en el que se detecta una amenaza de manera que la entidad central no pueda descifrar la agregación de valores cifrados, volviendo al esquema de funcionamiento normal inmediatamente después.

Aplicando el cifrado/descifrado bihomomórfico descrito de mediciones de consumo de energía generadas por medidores inteligentes, junto con la constitución de grupos de medidores inteligentes, el mecanismo de actualización de claves explicado y, cuando sea necesario, la “solución de testigos”, se logra un sistema en el que una entidad central, en particular un suministrador de energía, aun así puede beneficiarse de los informes (casi) instantáneos procedentes de medidores inteligentes para monitorizar, controlar y predecir mejor el uso de energía, en tanto que preservando la privacidad de los usuarios finales en cuanto a sus hábitos diarios en el hogar o sus pautas de utilización de aparatos, por ejemplo.

Existen varios modos de cómo diseñar y desarrollar con más detalle la enseñanza de la presente invención de un modo ventajoso. Con este fin, ha de hacerse referencia a las reivindicaciones de patente subordinadas respecto a la reivindicación de patente 1 por una parte, y a la siguiente explicación de un ejemplo preferido de una realización de la invención ilustrada por el dibujo por otra parte. En relación con la explicación del ejemplo preferido de una realización de la invención mediante la ayuda del dibujo, se explicarán realizaciones preferidas generalmente y desarrollos adicionales de la enseñanza. En los dibujos

La Fig. 1 es un diagrama que ilustra de manera ejemplar un perfil de carga de una casa unipersonal medido y el informe mediante un medidor inteligente según la técnica anterior,

la Fig. 2 ilustra esquemáticamente una realización de un procedimiento según la presente invención con dos grupos diferentes de medidores inteligentes, y

la Fig. 3 ilustra esquemáticamente una parte de una red de distribución inteligente en la que un escenario de actualización de claves de medidores inteligentes se ejecuta según una realización de la presente invención.

Con referencia a la Fig. 2, se ilustra un Suministrador de Energía (a partir de ahora, *ES*) que recibe mediciones de electricidad e_{ij} procedentes de una pluralidad de medidores inteligentes sm_i en el periodo *j*. En el escenario ilustrado en la Fig. 2, un objetivo es evitar que el *ES* conozca las mediciones individuales procedentes de los medidores inteligentes sm_i, sino sólo la agregación de estos. Además, un objetivo es evitar la figura de un agregador intermedio. Para hacerlo, el *ES* debe recibir todos los valores individuales cifrados, sin poder descifrarlos. Pero, una vez que se hace la agregación, debería, de hecho, poder descifrar tal valor agregado.

De acuerdo con la presente invención, los medidores inteligentes sm_i están “ocultos” dentro de grupos *G*, dos de los cuales se representan en la Fig. 1 - Grupo 1 y Grupo 2. Es decir, cada medidor inteligente sm_i toma su valor medido e_{ij}, lo cifra usando la clave k_{ij} y aplicando el esquema de cifrado *E*, y envía el valor cifrado $E_{kij}(e_{ij})$ al *ES*, a través de un canal seguro, ocultando así su identidad real como “un miembro del grupo *G(i)*”, en donde

$$E_{k_{ij}}(e_{ij}) = e_{ij} + k_{ij}\,.$$

De acuerdo con la presente invención, se emplea el esquema de cifrado bihomomórfico *E*, que es un esquema de cifrado simétrico que es homomórfico aditivo tanto en el espacio de texto sin cifrar como en el espacio de claves. Este tipo de cifrado permite que el *ES* descifre la agregación de informes cifrados, pero no esas mediciones cifradas individualmente. El agregador de claves sólo conoce las claves individuales, mientras que el *ES* sólo conoce tanto la clave agregada *K* como las mediciones cifradas individuales. Cabe destacar que cualquier mecanismo de cifrado bihomomórfico aditivo seguro con estas características puede usarse en el contexto de la presente invención.

En resumen, en la realización de la Fig. 2 se ejecutan las siguientes etapas, que en lo siguiente se describen para el Grupo 1:

1) Cada medidor inteligente del Grupo 1, sm_i^1, en el momento *j*, actualiza su clave k_{ij}^1 y la envía al agregador de claves. En el escenario de la Fig. 2, el medidor inteligente sm_3^1 está designado actualmente como agregador de claves, tal como se indica por la forma pentagonal del medidor inteligente.

2) El agregador de claves calcula la agregación de todas las claves recibidas según la siguiente ecuación:

$$K = f(k_1, k_2, ..., k_n) = \oplus_{i=1}^{n} k_i = \sum_{i=1}^{n} k_i\ ,$$

y envía tal clave agregada *K* al *ES*, tal como se ilustra por la línea discontinua. Esta etapa se realiza sólo una vez al principio o cada vez que un medidor inteligente del grupo abandona/falla o entra/se une al grupo. Si no es el principio, entonces el agregador de claves comprueba que la agregación de las claves recibidas k_{ij}^1 es igual a la clave agregada *K*, por coherencia.

3) Cada medidor inteligente sm_i^1 cifra su medición de consumo en el tiempo *j*, e_{ij}, usando su clave k_{ij}^1, dando como resultado $E_{k_{ij}}(e_{ij}^1)$.

4) El *ES* recibe las mediciones cifradas $E_{k_{ij}}(e_{ij}^1)\forall i$, es decir

$$(E_{k_{1j}}(e_{1j}^1), E_{k_{2j}}(e_{2j}^1), E_{k_{3j}}(e_{3j}^1), E_{k_{4j}}(e_{4j}^1))\,.$$

5) El *ES* calcula la agregación

$$\oplus_{i=1}^{n} E_{k_{ij}}(e_{ij}^1)$$

que sería igual a

$$E_K(\oplus_i e_{ij}^1)$$

a través del siguiente bihomomorfismo:

$$\oplus_{i=1}^{n} E_{k_{ij}}(e_{ij}^1) = \sum_{i=1}^{n} E_{k_{ij}}(e_{ij}^1) = \sum_{i=1}^{n}(e_{ij}^1 + k_{ij}^1) = \sum_{i=1}^{n} e_{ij}^1 + \sum_{i=1}^{n} k_{ij}^1 = \sum_{i=1}^{n} e_{ij}^1 + K = E_K(\oplus_{i=1}^{n} e_{ij}^1)$$

6) Después, el *ES* puede descifrar tal agregación por medio de la siguiente expresión:

$$D_K(\oplus_{i=1}^{n} E_{k_{ij}}(e_{ij}^1)) = D_K(E_K(\oplus_{i=1}^{n} e_{ij}^1)) = D_K\left(\sum_{i=1}^{n} e_{ij}^1 + K)\right) = \left(\sum_{i=1}^{n} e_{ij}^1 + K\right) - K = \sum_{i=1}^{n} e_{ij}^1 = \oplus_{i=1}^{n} e_{ij}^1$$

Un cifrado bihomomórfico es un cifrado que es homomórfico aditivo tanto en el espacio de texto sin cifrar como en el espacio de claves:

$$E_{k_1}(v_1) \oplus ... \oplus E_{k_a}(v_a) = E_{k_1 \oplus .. \oplus k_a}(v_1 + ... + v_a).$$

Tal como se mencionó anteriormente, este tipo de cifrado permite que el *ES* descifre la agregación de informes cifrados, pero no aquellas mediciones cifradas individualmente. El agregador de claves sólo conoce las claves individuales, mientras que el *ES* sólo conoce tanto la clave agregada *K* como las mediciones cifradas individuales.

En el caso improbable de tener una connivencia entre el agregador de claves actual (malicioso) y el *ES*, el primero podría enviar las claves individuales de los medidores inteligentes de su grupo al segundo, en lugar de enviar la agregación de tales claves. Entonces, el *ES* podría intentar todas las combinaciones posibles entre el conjunto de claves y el conjunto de valores cifrados individuales, intentando descifrar éstos. Sin embargo, como las claves individuales se actualizan cada ronda, y el agregador de claves se designa periódicamente, sería caro en cuanto a los cálculos requeridos (y probablemente no merecería la pena) para el *ES* actuar en connivencia con el agregador de claves y realizar tal ataque.

La Fig. 3 ilustra esquemáticamente un procedimiento de actualización para las claves empleadas por medidores inteligentes de un grupo específico según una realización de la presente invención. La actualización de claves se realiza por periodo de notificación de tal manera que la agregación de todas las claves del grupo, es decir, la clave agregada *K*, siempre permanece constante. Con este fin, los medidores inteligentes dentro del mismo grupo forman un “anillo” donde cada medidor inteligente envía al siguiente en el anillo un valor aleatorio, a través de un canal seguro, que se resta de su clave y se suma a la clave del siguiente medidor inteligente de la siguiente manera:

$$k_{i,j} = k_{i,j-1} - \delta_{i,j} + \delta_{i-1,j},$$

en la que *j* indica un periodo de notificación actual y *j-1* el periodo de notificación previo.

Muchas modificaciones y otras realizaciones de la invención expuesta en este documento vendrán a la mente de alguien experto en la materia a la que pertenece la invención que tiene el beneficio de las enseñanzas presentadas en la descripción precedente y los dibujos asociados. Por lo tanto, ha de comprenderse que la invención no ha de estar limitada a las realizaciones específicas desveladas y que la intención es que las modificaciones y otras realizaciones estén incluidas dentro del ámbito de las reivindicaciones adjuntas. Aunque en este documento se emplean términos específicos, se usan solamente en un sentido genérico y descriptivo y no a efectos de limitación.

REIVINDICACIONES

1. Procedimiento para operar una red de distribución inteligente que incluye una pluralidad de medidores inteligentes, estando configurados dichos medidores inteligentes para monitorizar al menos una cantidad física medida y para proporcionar resultados de medición de dicha al menos una cantidad física medida a una entidad central,

caracterizado por las siguientes etapas

dicha red de distribución inteligente es dividida en grupos *G* de medidores inteligentes sm_i, de manera que cada uno de dichos medidores inteligentes pertenece exactamente a un grupo,

todos los medidores inteligentes sm_i de uno de dichos grupos *G* cifran su valor medido e_i aplicando un esquema de cifrado bihomomórfico E_{ki} y lo envían a dicha entidad central,

un medidor inteligente por grupo es designado como agregador de claves al que todos los medidores inteligentes sm_i de ese grupo envían su clave k_i empleada para dicho cifrado,

dicho agregador de claves calcula la agregación de todas las claves recibidas k_i y envía la clave agregada *K* a dicha entidad central,

dicha entidad central agrega todos los valores medidos cifrados recibidos e_i y descifra dicha agregación empleando dicha clave agregada *K*.

2. Procedimiento según la reivindicación 1, en el que dicha al menos una cantidad física medida específica es el consumo de energía eléctrica de una unidad consumidora, en particular una casa.

3. Procedimiento según la reivindicación 1 o 2, en el que dicha entidad central es un suministrador de energía.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que dichos grupos *G* de medidores inteligentes sm_i son configurados metiendo en el mismo grupo los medidores inteligentes sm_i que pertenecen a un edificio específico, calle o pueblo.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que dichos medidores inteligentes sm_i notifican dicha al menos una cantidad física medida específica a dicha entidad central en intervalos de tiempo regulares.

6. Procedimiento según cualquiera de las reivindicaciones 1 a 5 en el que dichos medidores inteligentes sm_i notifican dicha al menos una cantidad física medida específica a dicha entidad central a través de un canal seguro,

en el que, preferentemente, se emplean firmas de grupo para establecer dicho canal seguro.

7. Procedimiento según cualquiera de las reivindicaciones 1 a 6, en el que el medidor inteligente sm_i que es designado como agregador de claves dentro de un grupo *G* se cambia de vez en cuando, y/o

en el que se realiza un cambio de dicho agregador de claves en caso de que un medidor inteligente sm_i que esté designado como agregador de claves falle, abandone el grupo *G* y/o actúe maliciosamente.

8. Procedimiento según cualquiera de las realizaciones 1 a 7, en el que dicho agregador de claves envía la clave agregada *K* a dicha entidad central a través de un canal seguro, y/o

en el que dicho agregador de claves envía la clave agregada *K* a dicha entidad central cada vez que un medidor inteligente sm_i del grupo *G* respectivo falla o abandona o entra en dicho grupo.

9. Procedimiento según cualquiera de las reivindicaciones 1 a 8, en el que se definen periodos de notificación *j* y en el que cada medidor inteligente sm_i usa una clave diferente k_{ij} por periodo de notificación para cifrar dicha al menos una cantidad física medida específica,

en el que dichas claves k_{ij} para cada periodo de notificación *j* pueden calcularse de tal modo que la clave agregada *K* de todos los medidores inteligentes sm_i de un grupo *G* permanece igual.

10. Procedimiento según la reivindicación 9, en el que los medidores inteligentes sm_i del mismo grupo *G* están compuestos como un anillo,

en el que cada medidor inteligente envía al medidor inteligente subsiguiente en dicho anillo un valor aleatorio $\delta_{i,j}$, y

en el que cada medidor inteligente sm_i, para establecer una nueva clave $k_{i,j}$ para un periodo de notificación subsiguiente *j*, resta de su clave $k_{i,j-1}$ empleada en al periodo de notificación precedente *j-1* el valor aleatorio $\delta_{i,j}$ enviado al siguiente medidor inteligente en dicho anillo y suma el valor aleatorio $\delta_{i-1,j}$ recibido desde el medidor inteligente precedente en dicho anillo.

11. Procedimiento según cualquiera de las reivindicaciones 1 a 10, en el que dicho agregador de claves, en el momento de recibir una clave procedente de un medidor inteligente sm_i, responde con un testigo de acuse de recibo.

12. Procedimiento según la reivindicación 11, en el que dicho medidor inteligente sm_i incluye dicho testigo de acuse de recibo dentro de su informe de dicha al menos una cantidad física medida específica a dicha entidad central,

en el que, preferentemente, dicha entidad central está configurada para rechazar el informe de medición procedente de medidores inteligentes sm_i que no incluyen dicho testigo.

13. Procedimiento según la reivindicación 12, en el que dicha entidad central, en el momento de recibir un informe de medición procedente de un medidor inteligente sm_i que incluye un testigo, responde a dicho agregador de claves con otro testigo,

en el que dicho agregador de claves, en el momento de recibir dicho testigo procedente de dicha entidad central, puede aceptar dicha clave recibida desde el medidor inteligente sm_i correspondiente.

14. Procedimiento según cualquiera de las reivindicaciones 11 a 13, en el que dichos testigos se añaden a los mensajes respectivos sólo en casos en los que dicha entidad central no puede descifrar los valores medidos cifrados agregados e_i.

15. Red de distribución inteligente, que incluye una pluralidad de medidores inteligentes, estando configurados dichos medidores inteligentes para monitorizar al menos una cantidad física medida y para proporcionar resultados de medición de dicha al menos una cantidad física medida a una entidad central
caracterizada porque

dicha red de distribución inteligente es dividida en grupos *G* de medidores inteligentes sm_i, de manera que cada uno de dichos medidores inteligentes pertenece exactamente a un grupo,

en la que todos los medidores inteligentes sm_i de uno de dichos grupos *G* están configurados para cifrar su valor medido e_i aplicando un esquema de cifrado bihomomórfico E_{ki} y enviarlo a dicha entidad central,

en la que un medidor inteligente por grupo *G* es designado como agregador de claves al que todos los medidores inteligentes sm_i de ese grupo envían su clave k_i empleada para dicho cifrado,

en la que dicho agregador de claves incluye medios para calcular la agregación de todas las claves recibidas k_i y para enviar la clave agregada *K* a dicha entidad central, y

en la que dicha entidad central está configurada para agregar todos los valores medidos cifrados recibidos e_i y para descifrar dicha agregación empleando dicha clave agregada *K*.

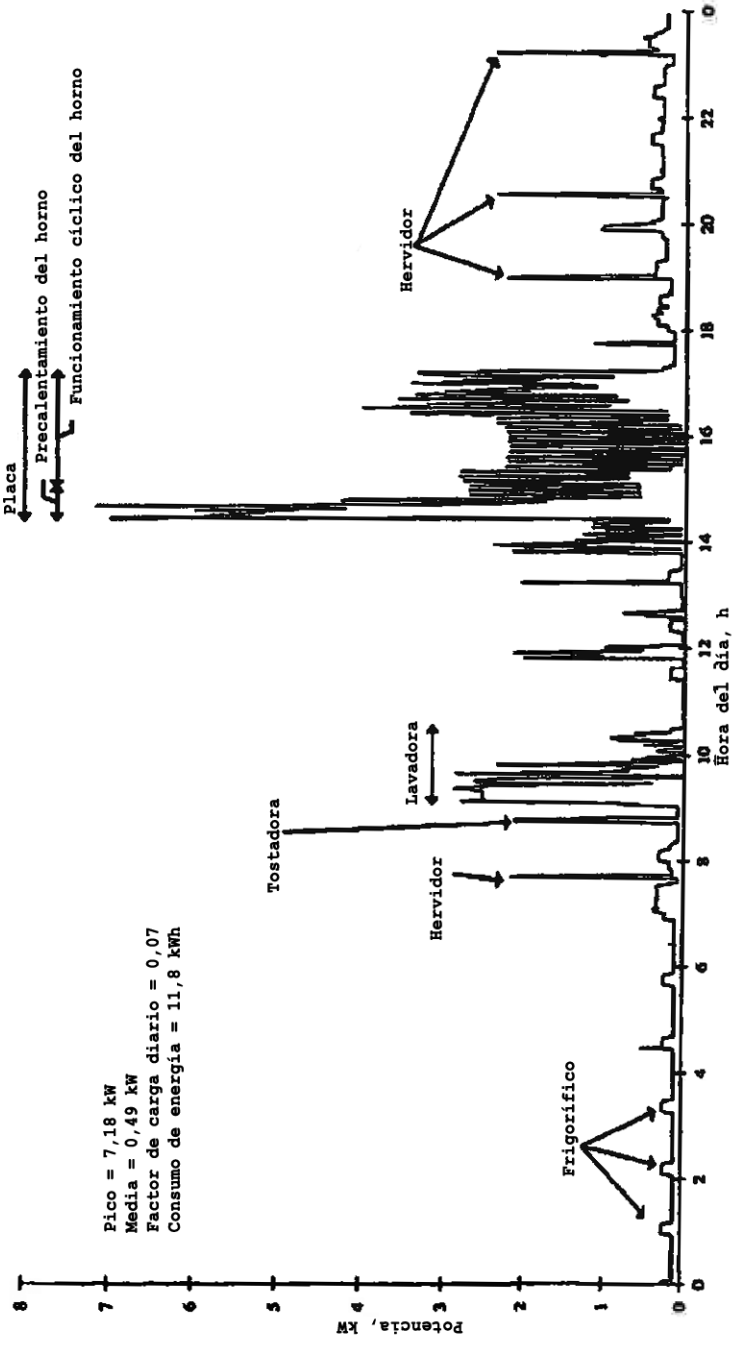
Placa
Precalentamiento del horno
Funcionamiento cíclico del horno
Pico = 7,18 kW
Media = 0,49 kW
Factor de carga diario = 0,07
Consumo de energía = 11,8 kWh
Frigorífico
Hervidor
Tostadora
Lavadora
Hervidor
Potencia, kW
Hora del día, h

Fig. 1

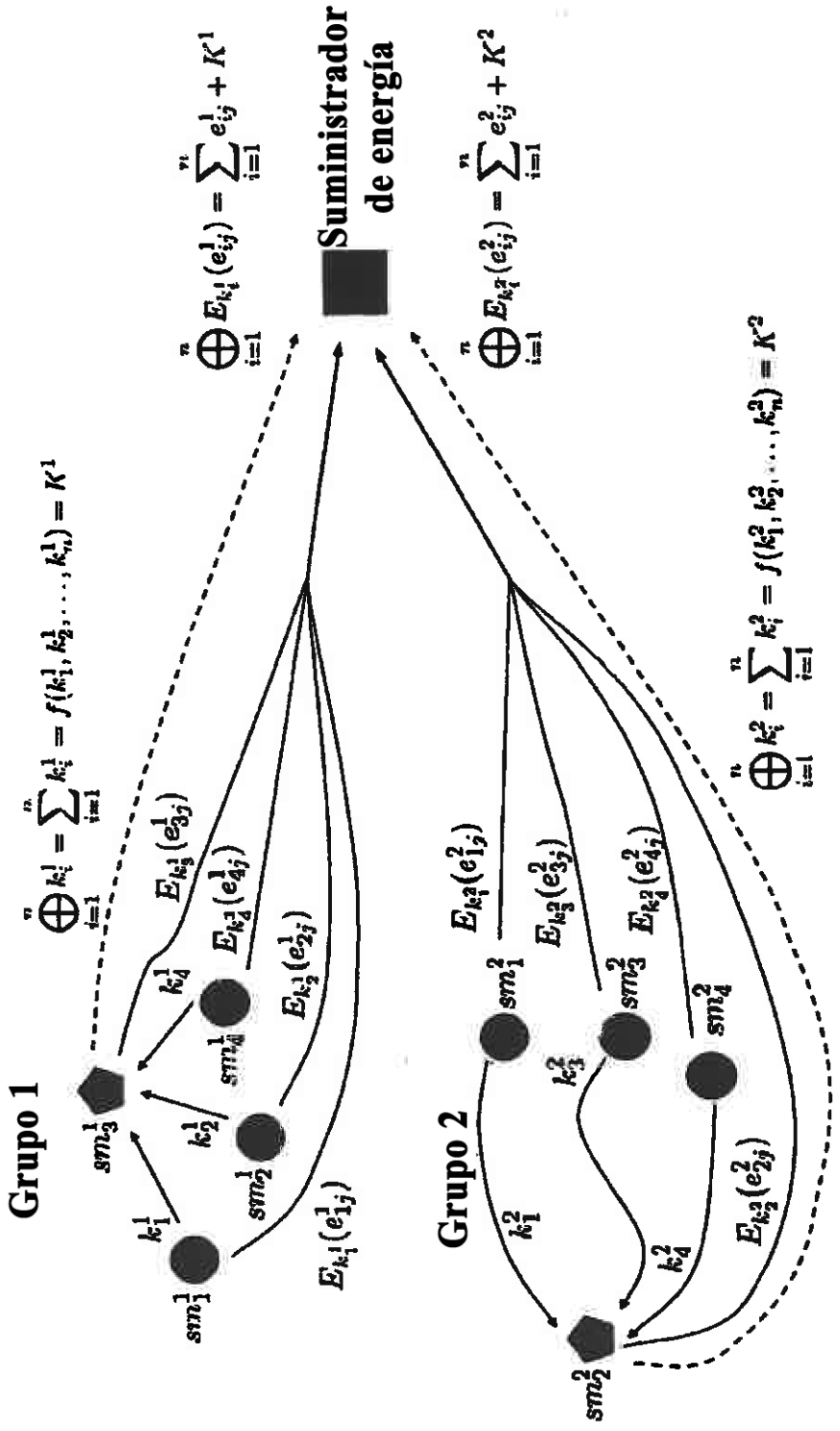

Fig. 2

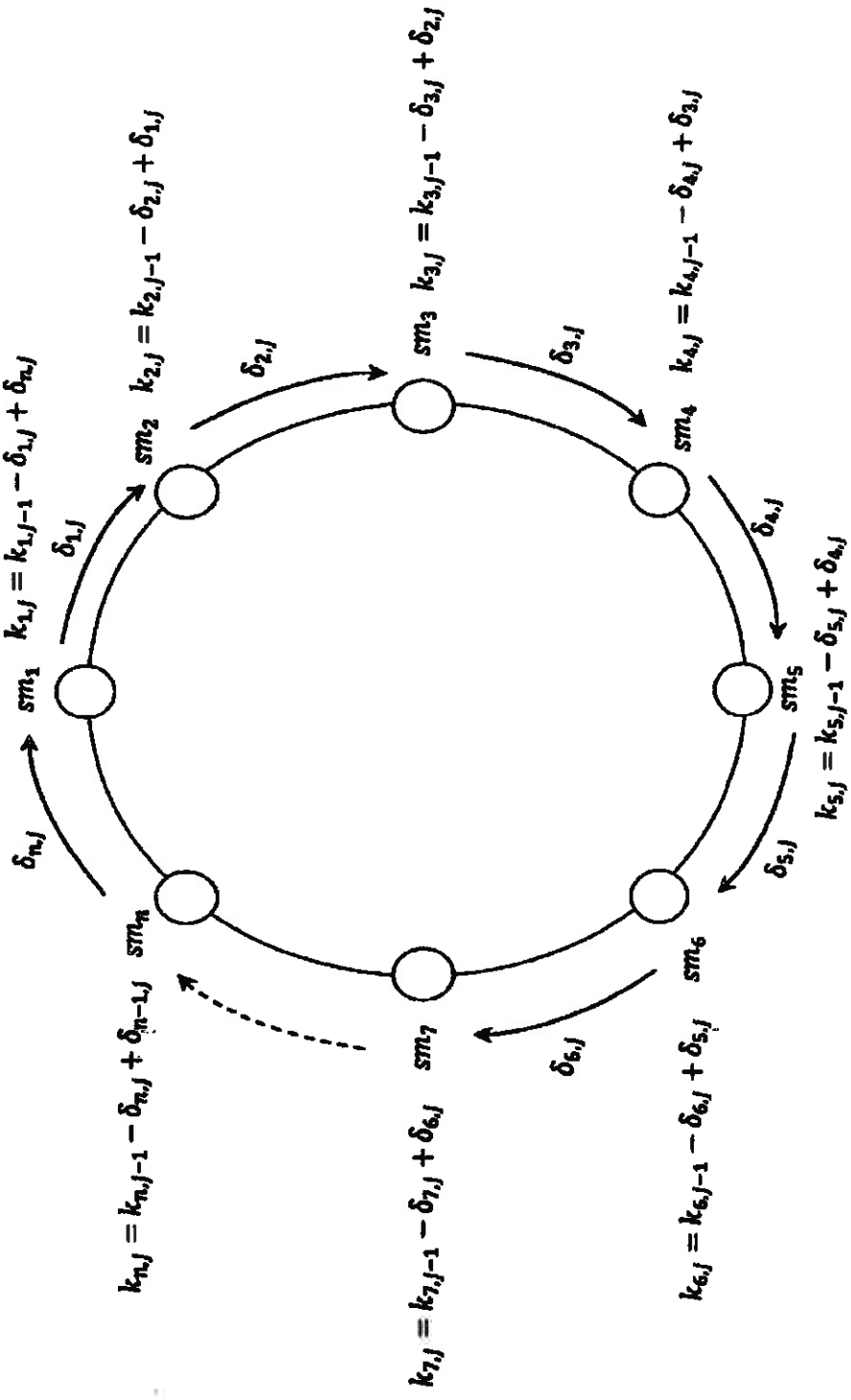
sm_1 $k_{1,j} = k_{1,j-1} - \delta_{1,j} + \delta_{n,j}$
sm_2 $k_{2,j} = k_{2,j-1} - \delta_{2,j} + \delta_{1,j}$
sm_3 $k_{3,j} = k_{3,j-1} - \delta_{3,j} + \delta_{2,j}$
sm_4 $k_{4,j} = k_{4,j-1} - \delta_{4,j} + \delta_{3,j}$
sm_5 $k_{5,j} = k_{5,j-1} - \delta_{5,j} + \delta_{4,j}$
sm_6 $k_{6,j} = k_{6,j-1} - \delta_{6,j} + \delta_{5,j}$
sm_7 $k_{7,j} = k_{7,j-1} - \delta_{7,j} + \delta_{6,j}$
sm_n $k_{n,j} = k_{n,j-1} - \delta_{n,j} + \delta_{n-1,j}$
$\delta_{1,j}$
$\delta_{2,j}$
$\delta_{3,j}$
$\delta_{4,j}$
$\delta_{5,j}$
$\delta_{6,j}$
$\delta_{n,j}$

Fig. 3