(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 530 625**

(51) Int. CI.:

G08G 1/054 (2006.01)
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.04.2012 E 12455003 (9)**

(97) Fecha y número de publicación de la concesión europea: **26.11.2014 EP 2648170**

(54) Título: **Método para detectar infracciones del límite de velocidad de un vehículo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2015

(73) Titular/es:

KAPSCH TRAFFICCOM AG (100.0%)
Am Europlatz 2
1120 Wien, AT

(72) Inventor/es:

ABL, ALEXANDER;
RASS, STEFAN;
SCHARTNER, PETER y
HORSTER, PATRICK

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método para detectar infracciones del límite de velocidad de un vehículo

La presente invención se refiere a un método para detectar infracciones de velocidad de un vehículo que se desplaza desde un primer sistema de carretera hasta un segundo sistema de carretera, también denominado "control de sección".

La expresión control de sección se refiere a un sistema técnico para la medición de las velocidades de los vehículos en los segmentos de carretera. Contrariamente a una trampa de velocidad estándar, que mide la velocidad de un vehículo que pasa en un punto determinado (por ejemplo, por medio de un Radar Doppler), un sistema de control de sección mide la velocidad media durante un cierto segmento de la carretera. Toma nota de un mismo vehículo que pasa por dos puntos geográficamente distantes dentro de un cierto tiempo. La distancia conocida de los dispositivos de medición, en lo sucesivo denominados sistemas o pórticos de carretera, en relación con el tiempo de desplazamiento conocido permite el cálculo de la velocidad media a lo largo de la sección de interés, y las acciones legales posteriores tras una infracción del límite de velocidad.

Cuando se implementa un sistema de control de sección, se tiene que prestar atención particular con respecto a la protección de la identidad del conductor de un vehículo observado. De hecho, el sistema debe respetar la privacidad del conductor hasta el punto en que haya evidencia de una infracción del límite de velocidad. En particular, esto significa que el sistema no debe almacenar o procesar datos personales para fines distintos a la detección de una infracción del límite de velocidad. Las identidades de los conductores que se han comportado correctamente deben ser protegidas en todo momento (es decir, ni almacenarse ni procesarse posteriormente).

Los métodos existentes para el control de sección (conf. por ejemplo, los documentos EP 2 220 634, EP 2 360 647) utilizan un esquema de cifrado basado en identidad IBE y se basan en la comparación de valores de comprobación de los identificadores de vehículos capturados en los sistemas de carretera, primero y segundo y, en caso de una coincidencia, evaluar sus marcas de tiempo de texto claro para calcular el tiempo de desplazamiento y, por lo tanto, la velocidad del vehículo entre el primer y el segundo sistemas de carretera. Cuando se detecta una infracción de la velocidad, los identificadores de vehículos capturados al principio tienen que recuperarse en los sistemas de carretera, primero y segundo, basados en los valores de comprobación, que requiere tablas de búsqueda adecuadas para los datos de evidencia capturados.

Todos los sistemas de la técnica anterior están todavía incompletos en materia de protección de datos y privacidad de los usuarios ya que el tiempo de desplazamiento de un vehículo es público, incluso cuando no hay infracción de la velocidad, y ya que los datos de evidencia originalmente capturados almacenados en los sistemas de carretera son propensos a ataques de intrusos.

Por lo tanto un objetivo de la presente invención es proporcionar un método para el control de sección con seguridad y privacidad mejoradas.

Para este fin, la invención proporciona un método para detectar una infracción de la velocidad de un vehículo que se desplaza desde un primer sistema de carretera hasta un segundo sistema de carretera, que comprende:

establecer parámetros públicos y privados, incluyendo una base de módulo común, de un esquema de cifrado basado en identidad (IBE) en un centro de generación de claves y los sistemas de carretera, primero y segundo;

capturar al menos un identificador de vehículo y una primera marca de tiempo en el primer sistema de carretera como primeros datos de evidencia, utilizar al menos el primer identificador y la primera marca de tiempo como una primera identidad para generar una primera clave pública de IBE, cifrar los primeros datos de evidencia con una primera clave de sesión aleatoria, cifrar la primera clave de sesión aleatoria con la primera clave pública de IBE, y suprimir los primeros datos de evidencia y la primera clave de sesión aleatoria en el primer sistema de carretera;

capturar al menos un identificador de vehículo y una segunda marca de tiempo en el segundo sistema de carretera como segundos datos de evidencia, utilizar al menos el segundo identificador y la segunda marca de tiempo como una segunda identidad para generar una segunda clave pública de IBE, cifrar los segundos datos de evidencia con una segunda clave de sesión aleatoria, cifrar la segunda clave de sesión aleatoria con la segunda clave pública de IBE, y suprimir los segundos datos de evidencia y la segunda clave de sesión aleatoria en el segundo sistema de carretera;

calcular una relación de las claves públicas, primera y segunda, modular la base de módulo común, y buscar la relación en una tabla de relaciones pre-calculadas para un conjunto de diferencias de tiempo entre dichas primera y segunda marcas de tiempo, conjunto que representa las infracciones de la velocidad, y, cuando la búsqueda es fructuosa:

recuperar al menos una clave privada de IBE para al menos una de dichas claves públicas de IBE desde el centro de generación de claves, descifrar al menos una de dichas claves de sesión cifradas con dicha clave privada, y descifrar al menos uno de dichos datos de evidencia cifrados con dicha clave de sesión descifrada.

Mediante la integración de las marcas de tiempo de los pasos de vehículos en los sistemas de carretera, primero y segundo, en las identidades, primera y segunda, de un esquema de cifrado de IBE, el tiempo de desplazamiento de un vehículo está completamente oculto en los casos en que no haya infracción de la velocidad, proporcionando mayor privacidad. El tiempo de desplazamiento solo se obtiene para los vehículos que han excedido el límite de velocidad y no para los demás.

La comparación de las claves públicas, primera y segunda, de IBE realiza un coincidencia de un identificador de vehículo combinado (por ejemplo, matrícula) y la comprobación de la infracción del límite de velocidad (diferencia de marca de tiempo) al mismo tiempo. Esto es una mejora notable con respecto a comprobación de dos etapas de la técnica anterior que comprueba primero la igualdad de los identificadores de vehículos y, tras una coincidencia, compara las marcas de tiempo.

Al mismo tiempo, utilizar el identificador de vehículo combinado y las identidades de marca de tiempo en un esquema de cifrado basado en identidad (IBE) guarda completamente las identidades en los sistemas de carretera y, por medio de las claves públicas basadas en los mismos, también los datos de evidencia subyacentes. Esto mejora drásticamente la seguridad en relación con ataques de intrusos a nivel de los sistemas de carretera. El centro de generación de claves central del esquema de IBE se puede proteger mejor con medidas criptográficas, técnicas y organizativas que los sistemas de carretera individuales lo que mejora la seguridad del sistema. Cada carretera puede cifrar de forma segura las identidades y datos de evidencia; solo un operario con acceso al centro de generación de claves puede descifrar los datos en caso de una infracción de la velocidad realmente verificado.

El método de la invención tiene también los siguientes beneficios:

1) cualquiera de los datos recogidos por un sistema de carretera se pueden utilizar solo en el sistema de carretera para determinar si se ha producido una infracción del límite de velocidad o no; no hay otra posibilidad semánticamente significativa o adicional de procesar y cifrar estos datos en un sistema de carretera;

2) los datos de evidencia relacionados con la identidad de un conductor nunca se almacenan de manera permanente y pueden ser destruidos inmediatamente y sin ningún rastro, si no se ha descubierto una infracción del límite de velocidad. El almacenamiento más allá de este punto de tiempo se permite solo para aquellos vehículos que han excedido, probadamente, el límite de velocidad;

3) durante el período de tiempo en que el vehículo está entre dos sistemas de carretera, el método asegura que no hay manera de extraer el identificador de vehículo (por ejemplo, número de matrícula o cualquier identidad del conductor) de los datos almacenados en el sistema;

4) es imposible descubrir que el mismo vehículo (incluso sin conocer su identificador) ha pasado varios sistemas de carretera, lo que impide que un enemigo tome perfiles de viajes.

En una realización preferida de la invención, el esquema de IBE es un esquema de cifrado Boneh-Franklin que está bien estudiado y tiene una alta fiabilidad.

Preferentemente, los datos de evidencia se pueden cifrar en el primer y/o segundos sistemas de carretera de acuerdo con un esquema de cifrado simétrico, en particular de acuerdo con el estándar de cifrado avanzado (AES), que garantiza una alta seguridad.

La seguridad contra el acceso de intrusos y los ataques de escucha se pueden mejorar aún más cuando los sistemas de carretera, primero y segundo, comparten al menos un valor aleatorio o pseudoaleatorio que se incorpora en la primera identidad para generar la primera clave pública de IBE y en la segunda identidad para generar la segunda clave pública de IBE. De esta manera dos sistemas de carretera se pueden "parear", y la clave pareada es un valor aleatorio o pseudoaleatorio que, opcionalmente, se puede cambiar de forma rutinaria. Para este fin, los sistemas de carretera, primero y segundo, se pueden comunicar para cambiar de forma síncrona de un valor pseudoaleatorio a un valor pseudoaleatorio posterior en una serie de valores pseudoaleatorios.

De acuerdo con una realización preferida adicional de la invención, la primera clave pública de IBE se genera en forma de:

$$PK_{1,j} := g^{((LPN|\,\mathrm{pad})\oplus R_j)\|t} \bmod p_G$$

con

$PK_{1,t}$ siendo la primera clave pública de IBE;
LPN t siendo el identificador y marca de tiempo de los primeros datos de evidencia;
R_i siendo el valor aleatorio o pseudoaleatorio;
g, p_G siendo los parámetros públicos del esquema de IBE;

y la segunda clave pública de IBE se genera en forma de:

$$PK_{2,t} := g^{(\{LPN\|\text{pad}\}\oplus R_i)\|i} \bmod p_G$$

$PK_{2,t}$ siendo la segunda clave pública de IBE;
LPN,t siendo el identificador y marca de tiempo de los segundos datos de evidencia;
R_i siendo el valor aleatorio o pseudoaleatorio; y
g, p_G siendo los parámetros públicos del esquema de IBE;

y la relación se calcula preferentemente en forma de:

$$PK_{2,t} \cdot PK_{1,t}^{-1} \pmod{p_G}$$

Estas operaciones se pueden implementar de manera eficaz, por ejemplo, mediante simples operaciones de transferencia de bits a nivel de bits, y están bien adaptadas para aplicaciones en tiempo real.

De acuerdo con otras realizaciones de la invención, los primeros datos de evidencia pueden comprender una imagen del vehículo tomada con una cámara en el primer sistema de carretera; y/o los segundos datos de evidencia pueden comprender una imagen del vehículo tomada con una cámara en el segundo sistema de carretera; y/o los primeros datos de evidencia se firman criptográficamente con una clave de firma del primer sistema de carretera; y/o los segundos datos de evidencia se firman criptográficamente con una clave de firma del segundo sistema de carretera.

En todas las variantes de la invención, las claves públicas, primera y segunda, de IBE, las claves de sesión cifradas, primera y segunda, y los datos de evidencia cifrados, primero y segundo, se pueden suprimir opcionalmente después de un período de tiempo predeterminado. Este período puede, por ejemplo, establecerse en el tiempo de desplazamiento máximo que tarda un vehículo con la velocidad de desplazamiento mínima para exceder la velocidad para desplazarse desde el primer hasta el segundo sistema de carretera.

En otras realizaciones de la invención, los primeros datos de evidencia pueden comprender una clase del vehículo capturado en el primer sistema de carretera. En este caso, las diferentes tablas de relaciones de claves públicas de IBE representativas de las infracciones de la velocidad se pueden pre-calcular para diferentes clases de vehículos, y la tabla utilizada para la búsqueda se elige en función de la clase del vehículo capturado.

Como alternativa o adicionalmente los primeros o segundos datos de evidencia pueden comprender una condición meteorológica o del camino capturada en el primer o segundo sistema de carretera, las diferentes tablas de relaciones se pre-calculan para diferentes condiciones meteorológicas o del camino, y la tabla utilizada para la búsqueda se elige de acuerdo con la condición meteorológica o del camino capturada.

Las etapas de calcular la relación de las claves públicas, primera y segunda, de IBE, la búsqueda posterior de la relación en la tabla de relaciones de pre-calculadas y todas las etapas adicionales en caso de una infracción de la velocidad se pueden realizar en cualquiera de los sistemas de carretera, primero y segundo. Para este fin, la primera clave pública de IBE se envía preferentemente al segundo sistema de carretera, o la segunda clave pública de IBE se envía al primer sistema de carretera, para calcular la relación.

Otros detalles, características y ventajas de la invención se harán evidentes a partir de la siguiente descripción de las realizaciones preferidas de la misma haciendo referencia a los dibujos adjuntos, en los que:

La Figura 1 es un diagrama de bloques de la arquitectura de alto nivel de los componentes utilizados en el método de la invención;

La Figura 2 es un diagrama de flujo de las etapas de preparación y cifrado de datos de evidencia en cualquiera de los sistemas de carretera, primero y segundo, dentro del método de la invención;

La Figura 3 es un diagrama de secuencia del método de la invención;

La Figura 4 es un diagrama de secuencia de la utilización y conmutación de valores pseudoaleatorios de una serie de valores pseudoaleatorios entre los sistemas de carretera, primero y segundo.

En el siguiente ejemplo, suponemos que los siguientes componentes e información estarán disponibles cuando se describe el sistema:

- La clase de vehículo (incluyendo vehículos de una sola vía y vehículos de dos vías).
- Las condiciones meteorológicas y del camino actuales, que determinan el límite de velocidad vigente para una clase de vehículo específico y una sección determinada.
- Relojes sincronizados en todo el sistema con una precisión de menos de 0,01 s.
- Los sistemas de carretera incluyen gabinetes de carretera para los equipos electrónicos, pórticos (o cualesquiera otras instalaciones para la fijación de cámaras, por ejemplo, puentes, bocas de túneles, postes, etc.) que están equipados con cámaras que son capaces de incorporar una marca de tiempo en la imagen. Además, suponemos que el sistema de carretera incluye una cámara para representar a través de una foto o bien proporcionar, de otra manera, la siguiente información:

    - La cara del conductor (en la medida en que la normativa legal lo permita).
    - Una identificación única tomada del sistema de carretera donde se ha tomado la imagen (es decir, una prueba del origen de la imagen).
    - La matrícula como identificador de vehículo.
    - Las condiciones meteorológicas y de tráfico actuales, incluyendo la posición y el carril de todos los vehículos pertinentes.
    - Un detector de la clase de vehículo.
    - Otra información tal como la ubicación geográfica, el identificador del sistema de carretera, carril y la dirección de conducción.

- La información antes mencionada se encuentra disponible de forma fiable para los vehículos que pasan por el sistema de carretera a una velocidad de hasta 250 km/h.

Además de estas hipótesis válidas para el sistema de carretera, suponemos adicionalmente las siguientes:

- Todas las conexiones entre las dos entidades en el sistema se protegen con SSL, es decir, se cifran y autentican. Se emplean algoritmos y longitudes de clave del estado de la técnica.
- Existe una autoridad central, el centro de generación de claves, que se protege por medidas criptográficas, técnicas y organizativas. En particular, todo el personal que trabaja dentro de este dominio de alta seguridad es de confianza y cualquier acceso físico a las respectivas instalaciones o datos están sujetos a al menos el principio de los cuatro ojos.
- Cualquier comunicación entre dos entidades en el sistema utiliza números de serie únicos para vincular las respuestas a las solicitudes respectivas (por lo tanto, no se menciona explícitamente el número de serie en los mensajes posteriores, y suponemos que está disponible de forma implícita).

La arquitectura de alto nivel (HLA) se muestra en la Figura 1. Sus componentes principales son los siguientes:

- Sistemas de carretera (RSS), que consisten en dos pórticos del sistema de carretera G_1 G_2, ambos de los que están equipados con cámaras. En cada uno de tales pórticos del sistema de carretera, suponemos que un dispositivo a prueba de manipulación (tal como un hardware dongle, tarjeta inteligente, elemento de confianza o criptoprocesador) está disponible.
- Operador (OP): esta es la única entidad del sistema que llega a ver toda la evidencia en referencia a una infracción del límite de velocidad sospechoso. Su deber es comprobar la exactitud de la presunta infracción y - en caso de una infracción – haciendo llegar la evidencia a las autoridades legales.
- Centro de generación de claves (KGC): el papel del centro de generación de claves está generando las claves de descifrado de la evidencia cifrada en una solicitud firmada por el operador. El hardware y el software necesario reside en un dominio de alta seguridad.
- Autoridades Legales: estas no son directamente parte del concepto técnico y, por lo tanto, no reciben mayor descripción en el presente documento.

Se describe el proceso general paso a paso, de acuerdo con los flujos de información que se muestran en las Figuras 1 - 3. El proceso comienza cuando un vehículo pasa el primer pórtico del sistema de carretera G_1.

1. El sistema de carretera en el pórtico G_1 percibe un vehículo y ejecuta las siguientes etapas:

    a. Recoge toda la información requerida de una posible acción legal. Esto incluye:

    - Una imagen *PIC* del vehículo. A partir de la imagen, se obtiene la matrícula *LPN* mediante el reconocimiento óptico de caracteres (OCR). Como alternativa, la matricula se puede ser reemplazar o aumentar por cualquier característica de identificación del vehículo (tales como señales de símbolos RFID, color, etc.). Sin pérdida de generalidad, nos referiremos a cualquier característica de identificación única de un vehículo como su "número de matrícula" en todo el resto del presente documento, aunque esto significa la identificación del vehículo en general.

- La clase de vehículo *VC* (coche, vehículo de carga pesada, etc.).
- Una marca de tiempo *t* (de acuerdo con los supuestos mencionados anteriormente, suponemos relojes sincronizados en todo el sistema).
- Datos adicionales *AD* según se requiera, por ejemplo, las condiciones meteorológicas y de camino actuales en la sección comprendida entre G_1 y G_2. Esta información respectiva se supone a disposición de ambos pórticos, G_1 y G_2.

A partir de sus datos recogidos, se crea el conjunto de datos evidencia como el registro *D = (LPN, t, VC, PIC, AD, Sig),* donde *Sig* es una firma digital de todos los datos de evidencia. Esto puede ser una Firma Rivest-Shamir-Adleman (RSA) estándar, tomando la clave de la firma SK_G del sistema de carretera clave para producir la *Sig* partir de los datos *(LPN, t, VC, PIC, AD).* Se puede comprobar por el operador quién tiene conocimiento auténticamente la clave pública respectiva PK_G del sistema de carretera. Esto es favorable para evitar los ataques que se basan en la presentación de datos de evidencia falsificados para el operador.

b. El sistema de carretera crea una nueva clave de sesión de 128 bits al azar $K \in \{0, 1\}^{128}$ y cifra *D* mediante AES (estándar de cifrado avanzado) proporcionando los datos cifrados *ED = AES (D, K*). Claves de sesión más largas son permisibles.

c. El sistema de carretera cifra la clave de sesión *K* por medio de un cifrado basado en identidad (IBE). Una realización del esquema de IBE es el esquema de cifrado Boneh-Franklin que se describe en D. Boneh y M. Franklin: Cifrado basado en Identidad de la pareja Weil, SIAM J. de Informática, 2003, 32, págs. 586-615; y L. Martin: Introducción al Cifrado basado en Identidad, Artech House, 2008. La respectiva clave pública $PK_{1,t}$ del esquema del IBE se crea (por ejemplo, dentro de un dispositivo a prueba de falsificaciones) como:

$$PK_{1,t} := g^{\{(LPN \| pad) \oplus R_i\} \| t} \bmod p_G \qquad (1)$$

donde ‖ denota la sencilla concatenación de cadena bits, y ⊕ es la operación XOR bit a bit. El parámetro p_G es un número primo que se selecciona suficientemente grande para asegurar que el problema del logaritmo discreto sea difícil (véase la Tabla 6). Las entradas y parámetros restantes son los siguientes:

- *g* es un elemento generador del esquema de IBE, aquí el elemento generador del grupo finito $Z^*_{p_G}$ (el conjunto de enteros modulan el p_G primo) con módulo de multiplicación p_G. Su longitud de bits se puede elegir como se recomienda en la Tabla 5.
- *pad* es cualquier cadena de relleno adecuada para obtener la longitud de bits deseada en el exponente. Ni su elección concreta ni su secreto tiene un impacto en la seguridad del sistema. Por lo tanto, se puede elegir un valor fijo en todo el sistema. En particular, todos los sistemas de carretera pueden utilizar el mismo relleno.
- *t* es la marca de tiempo UNIX (o POSIX) cuando el vehículo ha pasado por el pórtico del sistema de carretera. Este es el número de segundos transcurridos desde el Tiempo Universal Coordinado (UTC) a la medianoche del 1ero de enero de 1970, sin contar los segundos intercalares. Este valor está disponible, por defecto, en cualquier plataforma informática basada en Linux o UNIX.
- R_i es el generador de aleatoriedad actualmente válido (cadena de bits pseudoaleatorios) que cada sistema de carretera crea por sí solo. Este valor se puede ajustar individualmente y de forma independiente al azar para cada par de sistemas de carretera, y se puede cambiar periódicamente (véase a continuación). El XOR bit a bit de R_i con la matricula (y el relleno) frustra los ataques directos para revelar la identidad del conductor. Su generación y sincronización con su sistema de carretera próximo se describe más adelante.
  Destacamos explícitamente que el término generador de aleatoriedad de ahora en adelante se refiere a un valor (cadena de bits) pseudoaleatorio, en lugar del algoritmo que lo crea (siendo este último referido como un generador de números pseudoaleatorios).

Utilizar $PK_{1,t}$, el primer sistema de carretera de un par de sección cifra la clave de sesión para obtener *EK= IBE (K, $PK_{1,t}$).*

d. La clave de sesión *K* y los datos de evidencia *D* (que solo texto) se destruyen inmediatamente y permanentemente después su cifrado.

e. El sistema de carretera almacena temporalmente la clave de sesión cifrada *EK*, la clave pública $PK_{1,t}$ y los datos de evidencia *ED* cifrados en su almacenamiento (por ejemplo, disco duro). Dependiendo de la clase de vehículo y del límite de velocidad que se aplica en virtud de las condiciones meteorológicas y de camino actuales, todo este registro se destruye de forma permanente después de un período de unidades de tiempo Δ*T* (por ejemplo, segundos).
El "envejecimiento" de las claves públicas no requerirá una marca de tiempo absoluta, sino que puede implementarse con un contador que disminuye periódicamente y suprime tan pronto como llegue a cero (de manera similar a un campo del tiempo de vida).
Ejemplo (cálculo de Δ*T*): Supongamos que G_1 y G_2 están a 5 km de distancia y que el límite de velocidad es de 130 km/h en esta sección. En este caso, un vehículo no puede pasar G_2 antes que

$$\Delta T = \frac{5km}{130km/h} \cdot 3600 \approx 138{,}46s$$

después el mismo ha pasado G_1. De lo contrario, una infracción del límite de velocidad se debe haber producido.

El pórtico G_1 crea una lista de claves públicas para posteriores de solicitudes de búsqueda desde el pórtico G_2 (o viceversa). Esta lista se puede borrar las claves públicas obsoletas (almacenamiento temporal), es decir, aquellas que más viejas que ΔT Una clave se puede almacenar junto con el momento de su creación, es decir, un registro puede estar, por ejemplo, en forma de $(PK_{1,t},)$.

La Figura 2 muestra los detalles de la etapa 1 gráficamente. Por lo general, es conveniente realizar todas las operaciones criptográficas dentro del dominio del módulo de seguridad. Sin embargo, por razones de rendimiento, el cifrado AES y IBE se puede hacer *fuera* del módulo de seguridad (zona mostrada como una línea discontinua en la Figura 2), a condición de que la clave de sesión K sea destruida de forma fiable después del cifrado de los datos D y ocultándose a través del IBE.

2. El pórtico del sistema de carretera G_2 advierte un vehículo que pasa en un momento t (o después). Realiza los mismos pasos que G_1. Además, envía $(t, PK_{2,t})$, junto con los datos adicionales (clase de vehículo, las condiciones del camino, condiciones meteorológicas, etc.) según se requiera, a G_1, véase mensaje 1 (o viceversa). Como alternativa, es posible enviar solo la clave pública junto con un bit adicional (para indicar cuál generador de aleatoriedad se va a utilizar para la comprobación en el paso 3, véase a continuación, en un periodo de ΔT después de la conmutación), a fin de evitar el envío de una marca de tiempo (véase más adelante en los detalles).

3. Al momento $t' > t$, el sistema de carretera G_1 recibe $(t, PK_{2\,t})$ de G_2. El sistema de carretera G_1 filtra su lista de claves públicas y selecciona un conjunto de n entradas, que son relevantes para su comparación con $PK_{2,t}$. Denotamos esta lista (acortada y renombrada) como $\{PK_{1,1}, PK_{1,2},..., PK_{1,n}\}$. La comprobación se realiza mediante el cálculo

$$\begin{aligned} V &\equiv PK_{2,t} \cdot PK_{1,j}^{-1} \pmod{p_G} \\ &\equiv g^{[((LPN_2 \| \text{pad}) \oplus R_t) \| \mathbb{1}]} g^{-[((LPN_j \| \text{pad}) \oplus R_t) \| \mathbb{1}_j]} \pmod{p_G} \\ &\equiv g^{x \| y} \pmod{p_G} \end{aligned} \qquad (2)$$

para todos los índices $j = 1, 2,..., n,$ y donde y tiene la misma longitud de bits que las marcas de tiempo. Los productos $PK_{2,t} \cdot PK_{1,j}^{-1} \pmod{p_G}$ se pueden determinar utilizando las bibliotecas de programación estándares para el modulo aritmético y el valor resultante V se busca en una tabla pre-calculada.

La tabla de búsqueda pre-calculada almacena pares (V, tiempo de diferencia) de la forma que se muestran en la Tabla 1, donde ΔT es el tiempo para un desplazamiento de G_1 a G_2 a máxima velocidad para la clase de vehículo más lento permitido (por ejemplo, 139 segundos para una distancia de 5 kilómetros a una velocidad 130 km/h). Observe que la tabla 1 se puede *pre-calcular* y almacenar como una tabla de verificación (para su rápido acceso) en el hardware de los sistemas de carretera. Valores físicamente imposibles como 0 no necesitan incluirse en la tabla. Por otra parte, para un mejor rendimiento, se recomienda almacenar primero las diferencias de tiempo más probables y, por último, las diferencias de tiempo improbables cuando se llena la tabla inicialmente. Como alternativa, la búsqueda en la tabla de verificación se puede reemplazar por una búsqueda binaria dentro de una tabla pre-ordenada (a fin de conseguir tiempo de funcionamiento logarítmico para la búsqueda en tabla).

Tabla 1: Valores pre-calculados para la comprobación del límite de velocidad

V	Diferencia de Tiempo
g^0 MODp_g	0
g^1 MODp_g	1
g^2 MODp_g	2
⋮	⋮
$g^{\Delta T}$ MODp_g	ΔT

Por razones de eficacia, G_2 puede enviar $(t, PK_{2,t}^{-1})$ a G_1 y hacer que G_1 se calcule y buscar $PK_{2,t}^{-1} \cdot PK_{1,j}$ en su tabla (o viceversa). El contenido de la Tabla 1 tiene que modificarse en consecuencia.

- Si la búsqueda en tabla resulta negativa, es decir, el *valor* $V = PK_{2,t} \cdot PK_{1,j}^{-1}$ no se ha encontrado, entonces x‖y > ΔT. Esto indica que, o bien $x \neq 0$, de modo que $LPN_2 \neq LPN_j$, es decir, los números de la matrícula son diferentes, o de otro modo $x = 0$ (lo que significa matrículas idénticas) y $y = t - t_j > \Delta T$, de modo que no se ha producido una infracción del límite de velocidad. En cualquier caso, no hay ningún indicio de una infracción. En particular, esto significa que la comparación puede prácticamente nunca producir falsas alarmas negativas.

- Si la búsqueda en tabla resulta positiva, entonces el valor $V = g^t(x \| y)$ se ha encontrado, y el valor x‖y se puede obtener a partir de la búsqueda en tabla (columna "diferencia de tiempo"). Observe que la tabla solo puede almacenar los registros de diferencias de tiempo hasta ΔT. Observe que los generadores de generador de aleatoriedad dentro de PK_2 y $PK_{1,j}$. se pueden suponer idénticas en virtud de la sincronización (véase a continuación).
  Aproximamos la probabilidad de un falso positivo como sigue: Sea N el número de entradas en la Tabla 1. Este valor depende de ΔT (por ejemplo, para $\Delta T = 139$ segundos y una medición del tiempo con una precisión de 0,01 segundos, obtenemos $N \approx 13\,900$ entradas en la tabla). La probabilidad de un falso positivo es más o menos

$$\frac{N}{2^{longitudbit(p_G)}} = \frac{N}{2^{160}} \approx 10^{-44}$$

  y por tanto, insignificante. Así que en una búsqueda en tabla positiva, tenemos una evidencia abrumadoramente importante de que el mismo vehículo ha pasado los dos sistemas de carretera en un plazo más inferior a ΔT. Esto indica una infracción del límite de velocidad, que se puede transmitir a un operador para una segunda comprobación manual. Por lo que se refiere a la comprobación automática a través de la búsqueda en tabla, prácticamente no hay alarmas de falsos positivos.

4. Si se detecta una infracción del límite de velocidad de esta manera, entonces G_1 responde a G_2 en consecuencia, véase mensaje 2 en la Figura 1 (o viceversa, si la búsqueda en tabla se ha hecho en G_2), y ambos envían sus datos de evidencia cifrados ED_1, ED_2, las claves públicas PK_1, PK_2, las claves de sesión cifradas EK_1, EK_2 y el sistema los pórticos del sistema de carretera respectivos ID GID_1, GID_2 al operador. Los mensajes 3 en la Figura 1 (3a y 3b en la Figura 3) se envían desde G_i al operador, y son para $i = 1, 2$ - de la forma $(PK_i, EK_i, ED_i, GID_i, H(PK_1 \| PK_2))$, donde la última entrada $H(PK_1 \| PK_2)$ establece un enlace opcional entre los dos mensajes de ambos sistemas de carretera. La función H es una función de verificación segura criptográficamente. El operador puede reconocer tanto los mensajes mediante el envío de una corta notificación a los sistemas de carretera (para evitar que un enemigo bloquee esta conversación con el fin de ocultar una infracción del límite de velocidad).
La respuesta correcta de G_1 a G_2, el mensaje 2 (o viceversa) se forma mediante el envío $(PK_2, respuesta)$ con $respuesta \in \{sí, no\}$ a G_2, lo que asegura que G_2 se puede relacionar correctamente la respuesta a una búsqueda anterior (o viceversa).
5. El operador transmite (PK_1, PK_2) al centro de generación de claves y firma digitalmente toda su solicitud con su clave de firma secreta $SK_{sig\ op}$ (mensaje 4).
6. Tras una comprobación de firma fructuosa, el centro de generación de claves calcula las claves de descifrado SK_1, SK_2 que se refieren a PK_1, PK_2. Observe que estas claves de descifrado no existen en ninguna parte del sistema, ni antes de una sospecha de infracción del límite de velocidad. El centro de generación de claves cifra el registro (SK_1, SK_2) con la clave pública del operador PK_{op} y envía un texto cifrado RSA $C = RSA((SK_1, SK_2), PK_{op})$ al operador (mensaje 5).
7. El operador descifra C con su clave secreta SK_{op} y extrae SK_1, SK_2. Estas son necesarias para descifrar las claves de sesión EK_1, EK_2 para obtener las claves AES K_1, K_2, que se utilizan para descifrar los datos de evidencia D_1, D_2. Después de una comprobación manual para una infracción del límite de velocidad indicada correctamente los datos en la evidencia se pueden transmitir a las autoridades judiciales (mensaje 6).

La Figura 3 muestra todo el proceso como un diagrama de secuencia.

El proceso descrito hasta ahora se refiere a una única clase de vehículo y las condiciones de camino óptimas. Dependiendo de las condiciones meteorológicas y de la clase de vehículo, se pueden aplicar *diferentes límites de velocidad*. Esto equivale a utilizar un parámetro ΔT diferente al hacer la búsqueda en tabla a solicitud de G_2 (o G_1). Hay dos formas básicas para implementar esto:

1. Tabla de pre-cálculo 1 hasta ΔT máximo de todas las clases de vehículos, y hacer la búsqueda para obtener el tiempo real de desplazamiento (u obtener un "no encontrado" si el tiempo de desplazamiento fue mayor que el correspondiente al límite de velocidad más bajo en esta sección). Por ejemplo, si un vehículo de carga pesada está limitado a 60 km/h (dado $\Delta T_{HGS} = 300\ s$) y un coche puede conducir a velocidades de hasta 130 km/h (dado $\Delta T_{coches} = 138\ s$), a continuación, la tabla se calcula hasta valores $g^{\Delta T}$ con $\Delta T = max\{\Delta T_{HGS}, \Delta T_{coche}\} = 300\ s$. Esto determina el tamaño de la tabla, y la clase de vehículo (transmitido como datos adicionales en la búsqueda) se puede utilizar para decidir más tarde, si se ha producido realmente una infracción del límite de velocidad, si la búsqueda resulta positiva.
2. Como alternativa, una tabla de búsqueda diferente (Tabla 1) se puede calcular específicamente para cada clase de vehículo y límite de velocidad. En ese caso, la clase de vehículo transmitido determina qué tabla se utiliza para la búsqueda por RSS. Esto evita la comprobación adicional requerida por el enfoque de una sola tabla y es más rápido porque se tienen que registrar menos entradas para cada búsqueda. Por otra parte, esto oculta los tiempos de desplazamiento de los vehículos que se han encontrado en la tabla, pero que no han cometido una infracción del límite de velocidad con respecto a su clase de vehículo específica.

Durante la fase de configuración del sistema, cada par de sistemas de carretera (pórticos) pueden recibir opcionalmente un generador de aleatoriedad compartido es decir, un valor aleatorio o pseudoaleatorio. Para mayor seguridad, un generador de aleatoriedad particular, R_0 no debe ser compartido por más de dos sistemas de carretera.

Se debe prestar particular atención cuando se cambia el generador de generador de aleatoriedad. Llamemos al generador de generador de aleatoriedad inicial R_0 en ambos pórticos del sistema de carretera G_1, G_2 (establecido durante la inicialización del sistema). Dentro de, por ejemplo, un dispositivo a prueba de manipulaciones (como un hardware dongle, tarjeta inteligente, elemento de confianza, criptoprocesador, etc.), se genera el siguiente generador de aleatoriedad verificando el último, es decir, $R_{i+1} = H(R_i)$.

El generador de generador de aleatoriedad no debe dejar el dispositivo a prueba de manipulaciones ni ser accesible en modo alguno desde el exterior, por lo tanto, la ecuación (1) se debe evaluar dentro del dispositivo a prueba de manipulaciones. Almacenar el generador de generador de aleatoriedad externamente - si es necesario - se debe hacer criptográficamente.

La Tabla 2 en relación con la Figura 4 explica que generadores de generador de aleatoriedad se utilizan por G_1, G_2 para la creación de las claves públicas ("cifrar") y que generador de aleatoriedad se utiliza por G_1 (o G_2) en la búsqueda de su tabla de búsqueda tras la solicitud de G_2 (o G_1) ("comprobar").

Tabla 2: Uso de generador de aleatoriedad para la creación y comprobación de clave pública

Hora de llegada a pórtico del RSS G_1	**Hora de llegada al pórtico del RSS G_2**	
	Antes $t_{conmutación}$	Después $t_{conmutación}$
Antes $t_{conmutación}-\Delta T$	Caso (a) cifrar G_1:R, cifrar G_2:R comprobar R	Caso (b) cifrar G_1:R, cifrar G_2:R' comprobar: G_1 se comprobaría con R', pero ha suprimido la correspondiente clave pública en ese momento, por lo que no se ha producido infracción del límite de velocidad (tiempo de desplazamiento > ΔT)
Entre $t_{conmutación}-\Delta T$ y $t_{conmutación}$	Caso (c) cifrar G_1:R y R', cifrar G_2:R' comprobar: R	Caso (d) cifrar G_1:R y R', cifrar G_2:R' comprobar: R'
Después $t_{conmutación}$	imposible	Caso (e) cifrar G_1:R', cifrar G_2:R' comprobar: R'

La conmutación de los generadores de aleatoriedad se realiza preferentemente periódicamente, siempre que el período de validez de un generador de aleatoriedad sea mayor que ΔT a fin de evitar problemas de sincronización. Durante el inicio o después de una falta de corriente, G_1 y G_2 podrían utilizar una conexión SSL autenticada para acordar en secreto en un nuevo generador de aleatoriedad inicial R_0 e iniciar de nuevo la cadena de verificación. Esto se puede hacer mediante el protocolo estándar de estación a estación, tal como el intercambio de claves Diffie-Hellman. Sin embargo, esta sincronización "desde cero" podría sólo ser necesaria de vez en cuando, por ejemplo, después de una falta de corriente, y no tiene por qué suceder con mucha frecuencia. Como alternativa, un intercambio de claves manual (almacenamiento del nuevo R_0 en una tarjeta inteligente y su copia de la tarjeta inteligente en ambos RSS) después de una falta de corriente es también posible. Esto evita la necesidad de almacenar las claves criptográficas designadas para su sincronización en cada sistema de carretera.

Todo el tráfico del operador al KGC se puede firmar digitalmente. Tenga en cuenta que no está obligado a firmar digitalmente los mensajes 3 de los pórticos al operador, ya que cada sistema de carretera ha firmado sus datos de evidencia cifrada en primera instancia. Esto significa que ningún dato de evidencia falsificado será aceptado para su procesamiento por parte del operador. La respectiva clave de firma se puede almacenar en un dispositivo a prueba de manipulaciones. La clave secreta del operador está protegida con un código PIN para evitar que el enemigo que ha comprometido el hardware del operador tenga acceso a la clave, ya que la clave de firma del operador es inaccesible sin el PIN.

La gestión de claves relacionadas con SSL es hasta la implementación de pilas de protocolos SSL particular. Las longitudes de clave y algoritmos del estado de la técnica pueden ser empleados para este fin.

Para cada componente del sistema, la Tabla 3 enumera la clave que almacena, junto con la protección recomendada para la clave particular. Los parámetros del sistema de IBE se suponen auténticamente conocidos para cada componente.

Tabla 3: Resumen de claves criptográficas

Componente	Tecla/elemento de datos	Protección (Criptográfica)
Sistema de carretera	Clave de firma secreta SK_G	Confidencial (dentro de un dispositivo a prueba de manipulaciones)
Operador	Clave o claves públicas del sistema de carretera PK_G	Auténtica (certificada)
	Clave de firma secreta $SK_{sig\ op}$	Confidencial (dentro de un dispositivo a prueba de manipulaciones, está protegida con acceso de PIN
	Clave de descifrado secreta SK_{op}	Confidencial (igual que $SK_{sig\ op}$)
Centro de generación de claves	Clave de cifrado pública del operador PK_{op}	Auténtica (certificada)
	Clave de verificación de firma pública del operador $PK_{sig,\ op}$	Auténtica (certificada)

La Tabla 4 proporciona una lista de los parámetros del sistema, respectivas descripciones, propietarios y visibilidad de cada parámetro. Por razones de concisión, nos abstenemos de enumerar explícitamente los parámetros específicos para cada sistema de cifrado a cargo. Proponemos utilizar RSA y AES para cifrar los canales y utilizar el estándar de seguridad digital (DSS) para crear firmas digitales, aunque otros estándares de cifrado y autenticación conocidos en la técnica se podrían utilizar. Los parámetros respectivos se enumeran en la Tabla 4 implícitamente a través de la presencia de las respectivas claves públicas y secretas. Todos los parámetros, independientemente de su visibilidad, deben ser *auténticos* a lo sumo con la finalidad de frustrar los ataques basados en la manipulación de parámetros.

Tabla 4: Parámetros del sistema

Parámetro	Semántica y descripción	Propietario	Visibilidad
PK_G	Clave de firma pública de cada sistema de carretera. Se necesita para autenticar los datos presentados al operador para su verificación	Sistema de carretera (específico para cada pórtico)	Pública
SK_G	Clave de creación de firma secreta de un sistema de carretera. Se necesita para firmar digitalmente cualquier carga útil entregada al operador.	Sistema de carretera (específico para cada pórtico)	Secreta
PK_{op}	Clave de cifrado pública del operador. Utilizada por el KGC para suministrar secretamente una clave secreta tras una solicitud.	Operador	Pública
SK_{op}	Clave de descifrado secreta del operador. Se utiliza para descifrar la clave secreta cifrada para el IBE.	Operador	Secreta
$PK_{si,op}$	Clave de firma pública del operador. Se utiliza para verificar la autenticidad de las búsquedas en el KGC.	KGC	Pública
$SK_{si\ op}$	Clave de firma secreta del operador para autenticar búsquedas en el KGC.	Operador	Secreta
p_G	Un número primo para crear claves de cifrado dentro de un sistema de carretera	Sistema de carretera (el mismo para todos los pórticos cooperantes)	Pública
G	Elemento de generación del grupo finito $Z^*_{p_G}$ con multiplicación de modulo.	Cada) componente (cooperante en el sistema	Pública
Parámetros del sistema de IBE	Véase D. Boneh y M. Franklin, *Ic.*	Sistema de carretera (el mismo para todos los pórticos cooperantes) y el centro de generación de claves	Pública, a excepción de la llave maestra del KGC.

Le recomendamos los siguientes tamaños de clave y las limitaciones de parámetros de la Tabla 5, aunque no es obligatorio (*en general,* nos dicen que un número n tiene una longitud de bits t si $2^{t-1} \leq n < 2^t$).

Tabla 5: Tamaños de claves recomendados (parámetro de seguridad *t*)

Criptosistema	**Limitaciones de parámetros**
Cifrado RSA	*p, q* primos de longitud de bits mínima t = 2048 bits (recomendación NIST)
Firmas digitales DSA	*p, q*, primos donde *p* tiene una longitud de bits mínima *t* = 1024 bits y *q* tiene una longitud de bits mínima *t*= 160 bits
Cifrado basado en Identidad	*q* primo con el longitud de bits de al menos *t* = 160 bits
Grupo finito $Z^*_{p_G}$	p_G primo con longitud de bits de al menos *t* = 160 bits

En cuanto a lo que el cifrado basado en identidad (IBE) se refiere, además de los tamaños de clave recomendados anteriormente ninguna otra restricción en las curvas (tal como el número de clases mínimo u otros) utilizadas para las firmas digitales se aplican puesto que se trata de cifrado y no de firmas del esquema Boneh-Franklin. Sin embargo, le recomendamos los tamaños de clave utilizados para las firmas que se utilizarán, así como para el IBE.

Por lo general, es recomendable asegurarse de que el logaritmo discreto o problema de factorización en el grupo que estamos utilizando es firme. La *intensidad de cifrado b* mide los esfuerzos de factorizar un número entero o encontrar un logaritmo discreto, en comparación con una búsqueda directa sobre un conjunto de 2^b valores. Por lo tanto, un ejemplo de interpretar la Tabla 6 es el siguiente: La última fila de la tabla indica que encontrar un logaritmo discreto que modula un primo con un tamaño de al menos 256 bits (utilizando el algoritmo de Pollard, cf. A. Menezes, P.C. van Oorschot y S. Vanstone: Manual de criptografía aplicada, CRC Press LLC, 1997) es igualmente difícil, ya que la ruptura directa prueba todas la 2^{128} claves para un cifrado simétrico, o equivalentemente difícil como factorizar un número entero con 3072 bits. Al comparar los valores de la Tabla 5 con las recomendaciones dadas por la tabla 6, se recomiendan los últimos tamaños por seguridad, ya que estos están de acuerdo con las recomendaciones estandarizadas proporcionando, no obstante, una mejor seguridad a largo plazo:

Tabla 6: Intensidad criptográfica equivalente proporcionada por diferentes algoritmos

Intensidad de cifrado	Tamaño de grupo (primo)	Tamaño de entero o campo finito
80	160	1024
112	224	2048
128	256	3072
192	384	7168
256	512	15360

REIVINDICACIONES

1. Un método para detectar una infracción de la velocidad de un vehículo que se desplaza desde un primer sistema de carretera (G_1) hasta un segundo sistema de carretera (G_2), que comprende:

establecer parámetros públicos y privados (g, p_G), incluyendo una base de módulo común (p_G), de un esquema de cifrado basado en identidad (IBE) en un centro de generación de claves *(KGC)* y los sistemas de carretera, primero y segundo (G_1, G_2);
capturar al menos un identificador (*LPN*) del vehículo y una primera marca de tiempo (t) en el primer sistema de carretera (G_1) como primeros datos de evidencia (D), utilizar al menos el primer identificador (*LPN*) y la primera marca de tiempo (t) como una primera identidad para generar una primera clave pública de IBE ($PK_{1,t}$), cifrar los primeros datos de evidencia (D) con una primera clave de sesión aleatoria (K), cifrar la primera clave de sesión aleatoria (K) con la primera clave pública de IBE ($PK_{1,t}$), y suprimir los primeros datos de evidencia (D) y la primera clave de sesión aleatoria (K) en el primer sistema de carretera (G_1);
capturar al menos un identificador (*LPN*) del vehículo y una segunda marca de tiempo (t) en el segundo sistema de carretera (G_2) como segundos datos de evidencia(D), utilizar al menos el segundo identificador (*LPN*) y la segunda marca de tiempo (t) como una segunda identidad para generar una segunda clave pública de IBE ($PK_{2,t}$), cifrar los segundos datos de evidencia (D) con una segunda clave de sesión aleatoria (K), cifrar la segunda clave de sesión aleatoria (K) con la segunda clave pública de IBE ($PK_{2,t}$), y suprimir los segundos datos de evidencia (D) y la segunda clave de sesión aleatoria *(K)* en el segundo sistema de carretera (G_2);
calcular una relación (V) de las claves públicas, primera y segunda, ($PK_{1,t}$, $PK_{2,t}$), modular la base de módulo común (p_G), y buscar la relación (V) en una tabla de relaciones (V) pre-calculadas para un conjunto de diferencias de tiempo entre dichas primera y segunda marcas de tiempo (t), conjunto que representa las infracciones de la velocidad, y, cuando la búsqueda es fructuosa:

recuperar al menos una clave privada de IBE (SK_1, SK_2) para al menos una de dichas claves públicas de IBE ($PK_{1,t}$, $PK_{2,t}$) desde el centro de generación de claves (KGC), descifrar al menos una de dichas claves de sesión cifradas (EK) con dicha clave privada (SK_1, SK_2), y descifrar al menos uno de dichos datos de evidencia cifrados (ED) con dicha clave de sesión descifrada (K).

2. El método de la reivindicación 1, en el que el esquema de IBE es un esquema de cifrado Boneh-Franklin.

3. El método de las reivindicaciones 1 o 2, en el que los datos de evidencia (D) se cifran con la clave de sesión (K) de acuerdo con un esquema de cifrado simétrico.

4. El método de la reivindicación 3, en el que el esquema de encriptado simétrico es el estándar de cifrado avanzado (AES).

5. El método de cualquiera de las reivindicaciones 1 a 4, en el que los sistemas de carretera, primero y segundo, (G_1, G_2) comparten al menos un valor aleatorio o pseudoaleatorio (R_i) que se incorpora en la primera identidad para generar la primera clave pública de IBE ($PK_{1,t}$) y en la segunda identidad para generar la segunda clave pública de IBE ($PK_{2,t}$).

6. El método de la reivindicación 5, en el que la primera clave pública de IBE ($PK_{1,t}$) se genera en forma de:

$$PK_{1,t} := g^{(([LPN||\text{pad}) \oplus R_i)||s} \bmod p_G$$

con

$PK_{1,t}$	siendo la primera clave pública de IBE;
LPN t	siendo el identificador y la marca de tiempo de los primeros datos de evidencia;
R_i	siendo el valor aleatorio o pseudoaleatorio;
g, p_G	siendo los parámetros públicos del esquema de IBE;

y la segunda clave pública de IBE se genera en forma de:

$$PK_{2,t} := g^{(([LPN||\text{pad}) \oplus R_i)||s} \bmod p_G$$

con

$PK_{2,t}$	siendo la segunda clave pública de IBE;
LPN,t	siendo el identificador y la marca de tiempo de los segundos datos de evidencia;
R_i	siendo el valor aleatorio o pseudoaleatorio; y
g, p_G	siendo los parámetros públicos del esquema de IBE.

7. El método de la reivindicación 6, en donde la relación (*V*) se calcula en forma de:

$$PK_{2,t} \cdot PK_{1,t}^{-1} \left(\mathrm{mod}\, p_G\right).$$

8. El método de cualquiera de las reivindicaciones 5 a 7, en el que los sistemas de carretera primero y segundo, (G_1, G_2) se comunican para cambiar de forma sincrónica de un valor pseudoaleatorio (R_i) a un valor pseudoaleatorio posterior (R_i) en una serie de valores pseudoaleatorios (R_i).

9. El método de cualquiera de las reivindicaciones 1 a 8, en el que los primeros datos de evidencia (*D*) comprenden una imagen (*PIC*) del vehículo tomada con una cámara en el primer sistema de carretera (G_1), y los segundos datos de evidencia (*D*) comprenden una imagen (*PIC*) del vehículo tomada con una cámara en el segundo sistema de carretera (G_2).

10. El método de cualquiera de las reivindicaciones 1 a 9, en el que los primeros datos de evidencia (*D*) se firman criptográficamente con una clave de firma (SK_G) del primer sistema de carretera (G_1), y los segundos datos de evidencia (*D*) se firman criptográficamente con una clave de firma (SK_G) del segundo sistema de carretera (G_2).

11. El método de cualquiera de las reivindicaciones 1 a 10, en el que la clave de sesión (*K*) tiene al menos 128 bits.

12. El método de cualquiera de las reivindicaciones 1 a 11, en el que las claves públicas de IBE, primera y segunda, ($PK_{1,t}$, $PK_{2,t}$), las claves de sesión cifradas, primera y segunda (*EK*) y los datos de evidencia cifrados, primero y segundo, (*ED*) se suprimen después de un período de tiempo predeterminado (ΔT).

13. El método de cualquiera de las reivindicaciones 1 a 12, en el que los primeros datos de evidencia (*D*) comprenden una clase (*VC*) del vehículo capturada en el primer sistema de carretera (G_1).

14. El método de la reivindicación 13, en el que diferentes tablas de relaciones (*V*) se pre-calculan para diferentes clases (*VC*) de vehículos y la tabla utilizada para la búsqueda se elige de acuerdo con la clase capturada del vehículo.

15. El método de cualquiera de las reivindicaciones 1 a 14, en el que los primeros o segundos datos de evidencia (*D*) comprenden una condición meteorológica o del camino (*AD*) capturada en el primer o en el segundo sistemas de carretera (G_1, G_2), y en el que las diferentes tablas de relaciones (*V*) se pre-calculan para diferentes condiciones y la tabla utilizada para la búsqueda se elige de acuerdo con la condición capturada.

16. El método de cualquiera de las reivindicaciones 1 a 15, en el que la primera clave pública de IBE ($PK_{1,t}$) se envía al segundo sistema de carretera (G_2) o la segunda clave pública de IBE ($PK_{2,t}$) se envía al primer sistema de carretera (G_1) para calcular la relación (*V*).

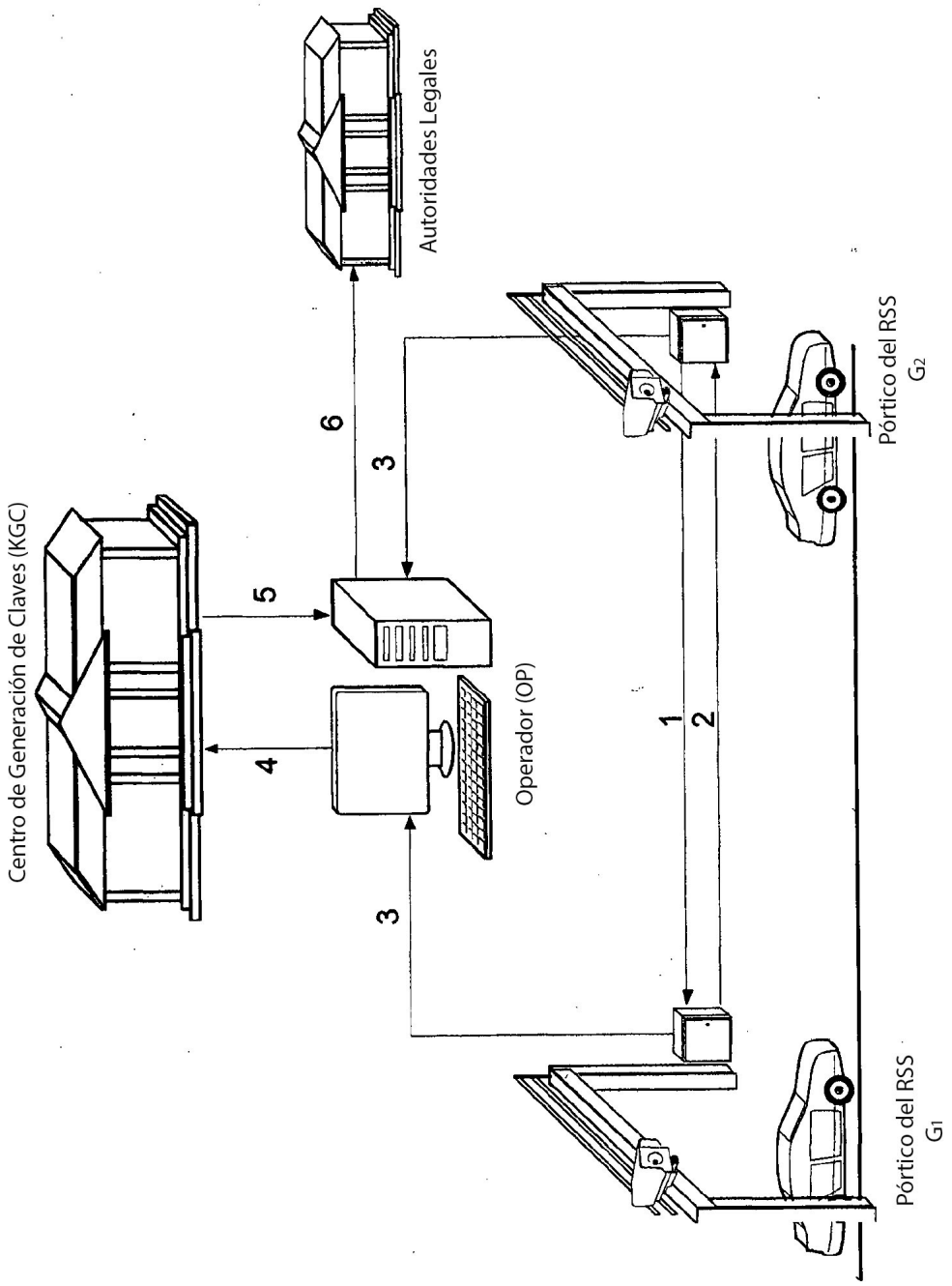
Autoridades Legales
Centro de Generación de Claves (KGC)
Operador (OP)
Pórtico del RSS G2
Pórtico del RSS G1
1
2
3
3
4
5
6

Fig. 1

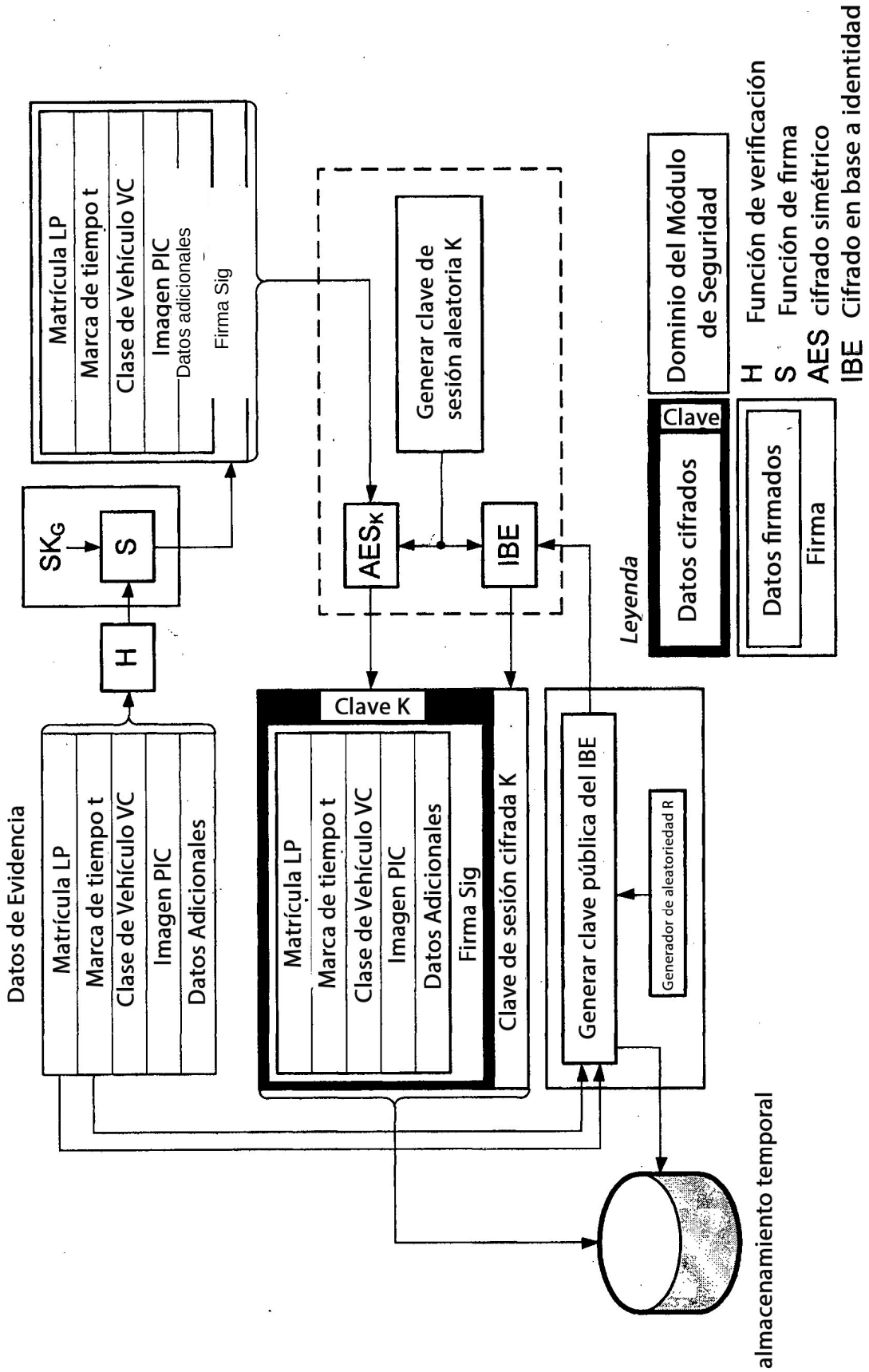
Datos de Evidencia
Matrícula LP
Marca de tiempo t
Clase de Vehículo VC
Imagen PIC
Datos Adicionales
H
SKG
S
Matrícula LP
Marca de tiempo t
Clase de Vehículo VC
Imagen PIC
Datos adicionales
Firma Sig
Generar clave de sesión aleatoria K
AESK
IBE
Clave K
Matrícula LP
Marca de tiempo t
Clase de Vehículo VC
Imagen PIC
Datos Adicionales
Firma Sig
Clave de sesión cifrada K
Generar clave pública del IBE
Generador de aleatoriedad R
almacenamiento temporal
Leyenda
Dominio del Módulo de Seguridad
Clave
Datos cifrados
Datos firmados
Firma
H Función de verificación
S Función de firma
AES cifrado simétrico
IBE Cifrado en base a identidad

Fig. 2

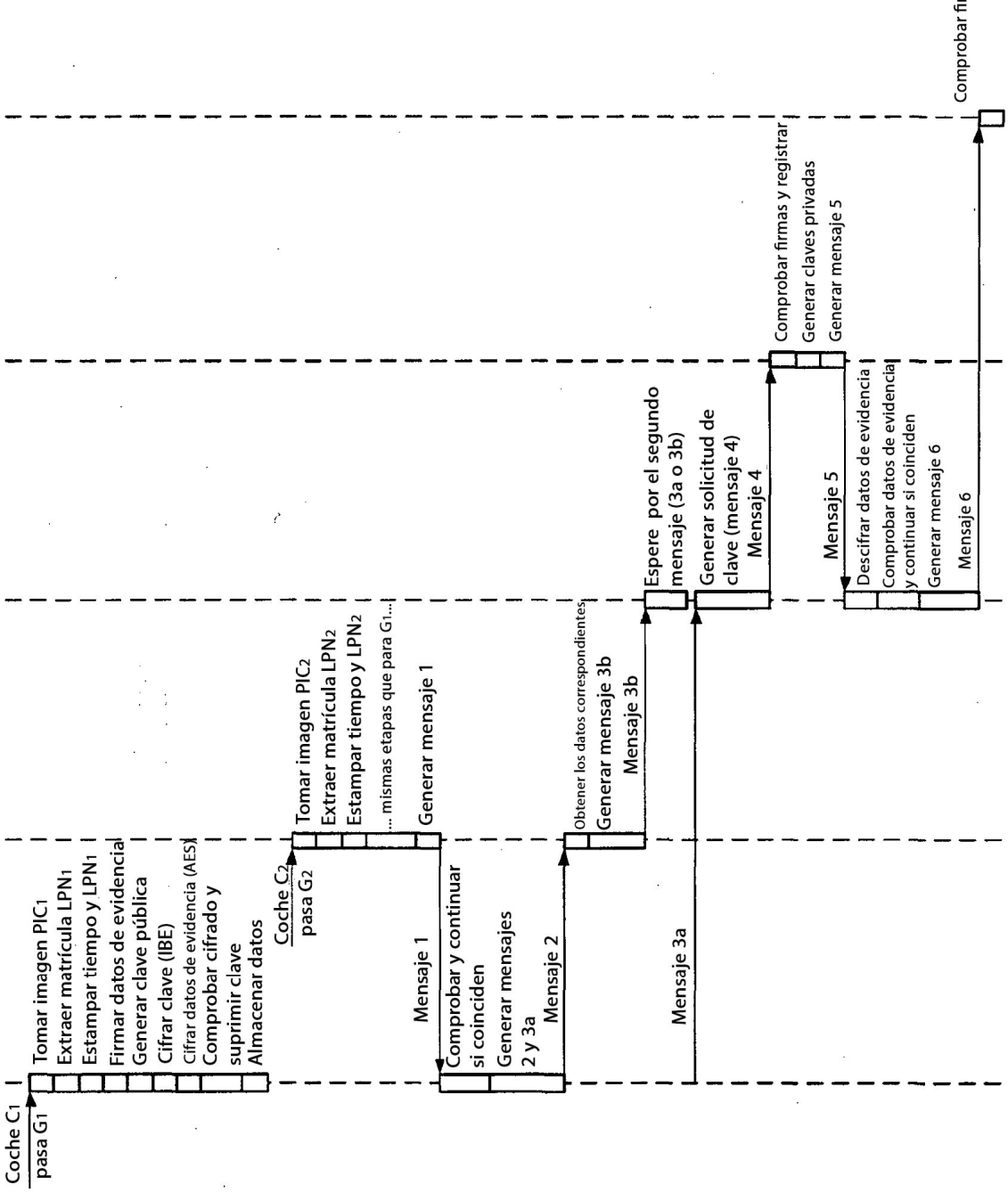
RSS G1
RSS G2
Operador OP
Centro de Generación de Claves KGC
Autoridades Legales LA
Coche C1 pasa G1
Tomar imagen PIC1
Extraer matrícula LPN1
Estampar tiempo y LPN1
Firmar datos de evidencia
Generar clave pública
Cifrar clave (IBE)
Cifrar datos de evidencia (AES)
Comprobar cifrado y suprimir clave
Almacenar datos
Coche C2 pasa G2
Tomar imagen PIC2
Extraer matrícula LPN2
Estampar tiempo y LPN2
... mismas etapas que para G1...
Generar mensaje 1
Mensaje 1
Comprobar y continuar si coinciden
Generar mensajes 2 y 3a
Mensaje 2
Obtener los datos correspondientes
Generar mensaje 3b
Mensaje 3b
Mensaje 3a
Espere por el segundo mensaje (3a o 3b)
Generar solicitud de clave (mensaje 4)
Mensaje 4
Comprobar firmas y registrar
Generar claves privadas
Generar mensaje 5
Mensaje 5
Descifrar datos de evidencia
Comprobar datos de evidencia y continuar si coinciden
Generar mensaje 6
Mensaje 6
Comprobar firmas y registrar

Fig. 3

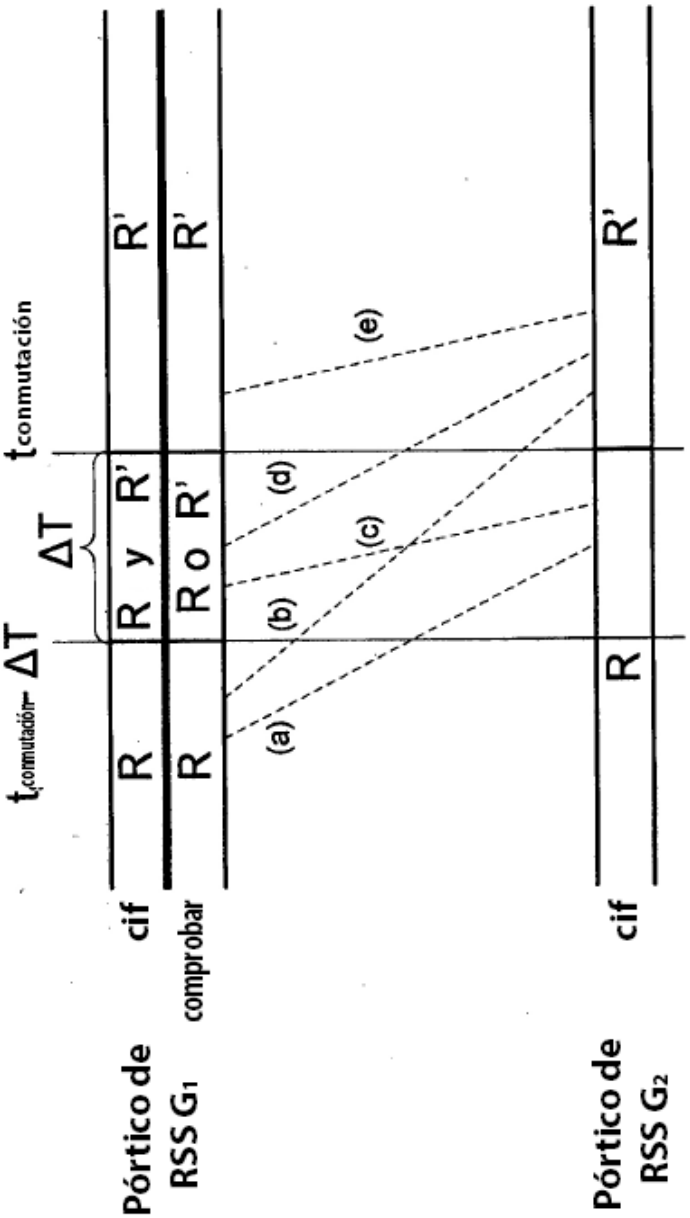
Pórtico de RSS G1
cif
comprobar
Pórtico de RSS G2
cif
R
R
R
R y R'
R o R'
R'
R'
R'
(a)
(b)
(c)
(d)
(e)
ΔT
ΔT
t conmutación
t conmutación

Fig. 4