(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 648 170 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
26.11.2014 Bulletin 2014/48

(21) Application number: **12455003.9**

(22) Date of filing: **06.04.2012**

(51) Int Cl.:
G08G 1/054 *(2006.01)* ***H04L 9/08*** *(2006.01)*
H04L 9/30 *(2006.01)* ***H04L 29/06*** *(2006.01)*

(54) **A method for detecting a speed violation of a vehicle**

Verfahren zur Detektion von Geschwindigkeitsüberschreitungen eines Fahrzeugs

Procédé permettant de détecter un excès de vitesse d'un véhicule

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(43) Date of publication of application:
09.10.2013 Bulletin 2013/41

(73) Proprietor: **Kapsch TrafficCom AG**
1120 Wien (AT)

(72) Inventors:
- **Abl, Alexander**
  9073 Viktring (AT)
- **Rass, Stefan**
  9020 Klagenfurt (AT)
- **Schartner, Peter**
  9020 Klagenfurt (AT)
- **Horster, Patrick**
  50226 Frechen (DE)

(74) Representative: **Weiser, Andreas**
Patentanwalt
Kopfgasse 7
1130 Wien (AT)

(56) References cited:
EP-A1- 2 360 647

EP 2 648 170 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to a method for detecting a speed violation of a vehicle traveling from a first roadside system to a second roadside system, also called "section control".

[0002] The term section control refers to a technical system for the measurement of speeds of vehicles on road segments. Contrary to a standard speed trap, which measures the speed of a bypassing vehicle at a certain point (e.g. by means of a Doppler-radar), a section control system measures the average speed over a certain road-segment. It takes notice of the same vehicle passing two geographically distant points within a certain time. The known distance of the measurement devices, hereafter called roadside systems or gantries, in connection with the known travel time permits calculation of the average speed along the section of interest, and subsequent legal actions upon a speed limit violation.

[0003] When a section control system is implemented, particular care has to be taken regarding the protection of the identity of an observed vehicle's driver. In fact, the system must respect the driver's privacy up to the point when there is evidence of a speed limit violation. In particular, this means that the system should not store or process any personal data for purposes other than detecting a speed limit violation. Identities of drivers that behaved correctly should be protected at all times (i.e. neither be stored or processed any further).

[0004] Existing methods for section control (conf. e.g. EP 2 220 634, EP 2 360 647) use an identity based encryption IBE scheme and rely on a comparison of hashed values of vehicle identifiers captured at the first and second roadside systems and, in case of a match, evaluating their clear-text timestamps to calculate travel time and thus the speed of the vehicle between the first and the second roadside systems. When a speed violation is detected, the vehicle identifiers captured at the outset have to be retrieved in the first and second roadside systems on the basis of the hashed values, which requires appropriate look-up tables for the captured evidence data.

[0005] All prior art systems are still incomplete regarding data protection and user privacy since the travel time of a vehicle is public, even when there is no speed violation, and since the originally captured evidence data stored in the roadside systems is prone to intruder attacks.

[0006] It is therefore an object of the present invention to provide a method for section control with improved security and privacy.

[0007] To this end, the invention provides for a method for detecting a speed violation of a vehicle traveling from a first roadside system to a second roadside system, comprising:

setting-up private and public parameters, including a common modulo basis, of an identity based encryption (IBE) scheme in a key generation center and the first and second roadside systems;

capturing at least an identifier of the vehicle and a first timestamp at the first roadside system as first evidence data, using at least the first identifier and first timestamp as a first identity to generate a first IBE public key, encrypting the first evidence data with a first random session key, encrypting the first random session key with the first IBE public key, and deleting the first evidence data and the first random session key at the first roadside system;

capturing at least an identifier of the vehicle and a second timestamp at the second roadside system as second evidence data, using at least the second identifier and second timestamp as a second identity to generate a second IBE public key, encrypting the second evidence data with a second random session key, encrypting the second random session key with the second IBE public key, and deleting the second evidence data and the second random session key at the second roadside system;

calculating a ratio of the first and second public keys, modulo the common modulo basis, and looking-up the ratio in a table of ratios pre-computed for a set of time differences between said first and second timestamps which set represents speed violations, and, when the look-up is successful:

retrieving at least one IBE private key for at least one of said IBE public keys from the key generation center, decrypting at least one of said encrypted session keys with said private key, and decrypting at least one of said encrypted evidence data with said decrypted session key.

[0008] By integrating the timestamps of the vehicle passages at the first and second roadside systems into the first and second identities of an IBE encryption scheme, the travel time of a vehicle is completely concealed in cases where there is no speed violation, providing enhanced privacy. The travel time is only obtained for vehicles that were violating the speed limit and not for others.

[0009] Comparing the first and second IBE public keys performs a combined vehicle identifier (e.g. license-plate) match and speed limit (timestamp difference) violation check in a single blow. This is a remarkable improvement over the prior art two-stage checks which first verify the equality of vehicle identifiers and upon a match compare the times-

tamps.

[0010] Concurrently, using combined vehicle identifier and timestamp identities in an identity based encryption (IBE) scheme completely seals the identities at the roadside systems and, by means of the public keys based thereon, also the underlying evidence data. This dramatically improves security over intruder attacks at the level of the roadside systems. The central key generation center of the IBE scheme can be better protected by cryptographic, technical and organizational measures than the individual roadsides systems which enhance system security. Each roadside can securely encrypt identities and evidence data; only an operator with access to the key generation center can decrypt the data in case of an actually verified speed violation.

[0011] The inventive method has also the following benefits:

1) any data collected by a roadside system is only usable in the roadside system for determining whether or not a speed limit violation has happened; there is no semantically meaningful other or further possibility of processing and encrypting this data in a roadside system;

2) evidence data related to a driver's identity is never stored permanently and can be destroyed immediately and without any traces if no speed limit violation has been discovered. Storage beyond this point in time is only permitted for those vehicles that have provably violated the speed limit;

3) for the period in time in which the vehicle is between two roadside systems, the method ensures that there is no way of extracting the vehicle identifier (e.g. license plate number or any drivers identity) from the data stored in the system;

4) it is impossible to discover that the same vehicle (even without knowing its identifier) has passed several roadside systems, which prevents an adversary from taking travel profiles.

[0012] In a preferred embodiment of the invention the IBE scheme is a Boneh-Franklin encryption scheme which is well-studied and has high reliability.

[0013] Preferably, the evidence data can be encrypted at the first and/or second roadside system according to a symmetric encryption scheme, in particular according to the advanced encryption standard (AES), ensuring high security.

[0014] Security against intruder access and eavesdropping attacks can be further improved when the first and second roadside systems share at least one random or pseudorandom value which is incorporated into the first identity to generate the first IBE public key and into the second identity to generate the second IBE public key. In this way two roadside systems can be "paired", and the pairing key is a random or pseudorandom value which can optionally be changed routinely. To this end the first and second roadside systems can communicate to synchronously switch from one pseudorandom value to a subsequent pseudorandom value in a series of pseudorandom values.

[0015] According to a further preferred embodiment of the invention the first IBE public key is generated in the form

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

with

$PK_{1,t}$ being the first IBE public key,
LPN, t being the identifier and timestamp of the first evidence data,
R_i being the random or pseudorandom value,
g, p_G being public parameters of the IBE scheme,

and the second IBE public key is generated in the form

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

with

$PK_{2,t}$ being the second IBE public key,
LPN, t being the identifier and timestamp of the second evidence data,

R_i being the random or pseudorandom value, and
g, p_G being public parameters of the IBE scheme;

and the ratio is preferably calculated in the form

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

[0016] These operations can be implemented efficiently, e.g. by simple bit shifting operations on bit level, and are well-suited for realtime applications.

[0017] According to further embodiments of the invention, the first evidence data may comprise a picture of the vehicle taken with a camera at the first roadside system; and/or the second evidence data may comprise a picture of the vehicle taken with a camera at the second roadside system; and/or the first evidence data is cryptographically signed with a signature key of the first roadside system; and/or the second evidence data is cryptographically signed with a signature key of the second roadside system.

[0018] In all variants of the invention the first and second IBE public keys, the encrypted first and second session keys and the encrypted first and second evidence data can be optionally deleted after a predetermined period of time. This period can e.g. be set to the maximum travel time it takes for a vehicle with minimum speed-violating travel speed to travel from the first to the second roadside system.

[0019] In further embodiments of the invention the first evidence data may comprise a class of the vehicle captured at the first roadside system. In this case, different tables of IBE public key ratios representative of speed violations can be pre-computed for different classes of vehicles, and the table used for the look-up is chosen according to the captured class of the vehicle.

[0020] Alternatively or additionally the first or second evidence data may comprise a weather or road condition captured at the first or second roadside system, different tables of ratios are pre-computed for different weather or road conditions, and the table used for the look-up is chosen according to the captured weather or road condition.

[0021] The steps of calculating the ratio of the first and second IBE public keys, the subsequent looking-up of the ratio in the pre-computed ratio table and all further steps in case of a speed violation can be performed in either of the first and second roadside systems. To this end, preferably the first IBE public key is sent to the second roadside system, or the second IBE public key is sent to the first roadside system, for calculating the ratio.

[0022] Further details, features and advantages of the invention will now become apparent from the following description of preferred embodiments thereof under reference to the accompanying drawings, in which:

Fig. 1 is a block diagram of the high level architecture of the components used in the method of the invention;

Fig. 2 is a flowchart of evidence data preparation and encryption steps in either of the first and second roadside systems within the method of the invention;

Fig. 3 is a sequence diagram of the method of the invention;

Fig. 4 is a sequence diagram of the usage and switching of pseudorandom values of a pseudorandom values series between the first and second roadside systems.

[0023] In the example below, we assume the following components and information to be available when describing the system:

- The vehicle class (including single-track and two-track vehicles).
- The current weather and road-conditions, which determine the currently valid speed limit for a specific vehicle class and a given section.
- Synchronized clocks throughout the system with a precision of less than 0.01 sec.
- The roadside systems include roadside cabinets for the electronic equipment, gantries (or any other facilities to affix cameras, e.g. bridges, tunnel portals, poles etc.) which are equipped with cameras that are capable of embedding a time-stamp in the picture. In addition, we assume the roadside system including a camera to either display via a photo or otherwise provide the following information:

    o The face of the driver (insofar legal regulations permit this).
    o A unique identification token of the roadside system where the picture has been taken (i.e. a proof of origin

of the picture).
o The license-plate number as vehicle identifier.
o The current traffic and weather conditions, including the position and lane of all relevant vehicles.
o A vehicle class detector.
o Other information like the geographical location, roadside system identifier, lane and direction of driving.

- The aforementioned information is available reliably for vehicles passing the roadside system at a speed of up to 250 km/h.

[0024] Besides these hypotheses valid for the roadside system, we additionally assume the following:

- All connections between any two entities in the system are SSL-protected, i.e. encrypted and authenticated. State-of-the-art algorithms and key-lengths are employed.
- A central authority, the key-generation center, exists that is protected by cryptographic, technical and organizational measures. In particular, any staff working within this high-security domain is trustworthy and any physical access to the respective facilities or data is subject to at least a four-eyes principle.
- Any communication between any two entities in the system uses unique serial numbers to link answers to respective requests (we therefore not explicitly mention the serial number in the subsequent messages and assume it available implicitly).

[0025] The high-level architecture (HLA) is displayed in Figure 1. Its main components are the following:

- Roadside systems (RSS): these consist of two roadside system gantries G_1 G_2, both of which are equipped with cameras. In each such roadside system gantry, we assume a tamper-proof device (such as a hardware dongle, smartcard, trusted element or cryptoprocessor) available.
- Operator (OP): this is the only entity in the system that gets to see the entire evidence referring to a speed limit violation suspect. Its duty is checking the correctness of the suspected violation and - in case of a violation - passing the evidence onwards to the legal authorities.
- Key generation center (KGC): the key generation center's role is generating the decryption keys for the encrypted evidence upon a signed request from the operator. The necessary hardware and software resides in a high-security domain.
- Legal Authorities: these are not directly part of the technical concept and therefore receive no further discussion in this document.

[0026] We describe the overall process step-by-step, according to the information flows displayed in Figs. 1 - 3. The process starts when a vehicle passes the first roadside system gantry G_1.
1. The roadside system at gantry G_1 notices a vehicle and executes the following steps:

a. Collect all information required for potential legal action. This includes:

- A picture *PIC* of the vehicle. From the picture, it obtains the license-plate number *LPN* by means of optical character recognition (OCR). Alternatively, the license-plate number can be replaced or augmented by any identification feature of the vehicle (such as signals from RFID-tokens, color, etc.). Without loss of generality, we shall refer to any unique identification feature of a vehicle as its "license-plate number" throughout the remainder of this document, although this means the vehicle identifier in general.
- The vehicle class *VC* (car, heavy-goods vehicle, etc.).
- A timestamp *t* (according to the assumptions stated above, we assume synchronized clocks throughout the entire system).
- Additional data *AD* as required, e.g. the current weather- and road-conditions on the section between G_1 and G_2. This respective information is assumed available to both gantries, G_1 and G_2.

From its collected data, it creates the evidence dataset as the record $D = (LPN, t, VC, PIC, AD, Sig)$, where *Sig* is a digital signature of all evidence data. This can be a standard Rivest-Shamir-Adleman (RSA)-signature, taking the roadside system's secret signature key SK_G to produce *Sig* from the data (LPN, t, VC, PIC, AD). It can be verified by the operator who authentically knows the respective public key PK_G of the roadside system. This is favourable to avoid attacks which are based on submitting faked evidence data to the operator.

b. The roadside system creates a fresh random 128 Bit session key $K \in \{0, 1\}^{128}$ and encrypts *D* by means of AES

(advanced encryption standard) giving the encrypted data *ED = AES (D, K*). Longer session keys are permissible.

c. The roadside system encrypts the session key *K* by means of identity-based encryption (IBE). An embodiment of the IBE scheme is the Boneh-Franklin encryption scheme described in D. Boneh and M. Franklin: Identity based encryption from the Weil pairing, SIAM J. of Computing, 2003, 32, pp. 586-615; and L. Martin: Introduction to Identity-Based Encryption, Artech House, 2008. The respective public key $PK_{1,t}$ of the IBE scheme is created (e.g. within a tamper-proof device) as:

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

where $\|$ denotes the simple bitstring-concatenation, and $\oplus$ is the bitwise XOR-operation. The parameter p_G is a prime number that is selected sufficiently large to ensure that the discrete logarithm problem is hard (see Table 6). The remaining inputs and parameters are as follows:

- *g* is a generating element of the EBE scheme, here the generating element of the finite group $Z^*_{p_G}$ (the set of integers modulo the prime p_G) with multiplication modulo p_G. Its bit-length can be chosen as recommended in Table 5.
- *pad* is any suitable padding string to get the desired bit-length in the exponent. Neither its concrete choice nor its secrecy has an impact on the security of the system. Hence, this value can be chosen fixed throughout the entire system. In particular, all roadside systems can use the same padding.
- *t* is the UNIX (or POSIX) time-stamp when the vehicle passed the roadside system gantry. This is the number of seconds elapsed since midnight coordinated universal time (UTC) of January 1st 1970, not counting leap seconds. This value is by default available on any UNIX- or Linux-based computing platform.
- R_i is the currently valid randomizer (pseudorandom bitstring) that each roadside system creates on its own. This value can be set individually and independently random for each pair of roadside systems, and can be changed periodically (see below). The bitwise XOR of R_i with the license-plate number (and padding) thwarts brute-force attacks to disclose the driver's identity. Its generation and synchronization with its neighboring roadside system is discussed later on.
  We explicitly remark that the term randomizer henceforth refers to a pseudorandom *value* (bitstring), rather to the algorithm that creates it (the latter being referred to as a pseudorandom number generator).

Using $PK_{1,t}$, the first roadside system of a section pair encrypts the session key to obtain *EK = IBE (K, $PK_{1,t}$)*.

d. The session-key *K* and the evidence data *D* (it's plain text) are destroyed immediately and permanently after encrypting it.

e. The roadside system temporarily stores the encrypted session key *EK*, the public key $PK_{1,t}$ and the encrypted evidence data *ED* in its storage (e.g. harddisk). Depending on the vehicle class and the speed limit that applies to it under the current weather and road-conditions, this entire record is permanently destroyed after a period of ΔT time units (e.g. seconds).
The "aging" of public keys does not require an absolute timestamp, but can be implemented with a counter that is decremented periodically and deleted as soon as it reaches zero (similarly to a time-to-live field).
Example (calculation of ΔT): Assume that G_1 and G_2 are 5 km apart and that the speed limit is 130 km/h on this section. In this case, a vehicle may not pass G_2 sooner than

$$\Delta T = \frac{5km}{130km/h} \cdot 3600 \approx 138.46s$$

after it has passed G_1. Otherwise, a speed limit violation must have occurred.

Gantry G_1 creates a list of public keys for subsequent look-up requests from gantry G_2 (or vice versa). This list can be cleared from outdated public-keys (temporal storage), i.e. those which are older than ΔT A key can be stored along with the time of its creation, i.e. a record can be e.g. of the form *($PK_{1,t}$)*.
Figure 2 displays the details of step 1 graphically. It is, in general, advisable to perform all cryptographic operations within the security module domain. However, for performance reasons, AES- and IBE-encryption can be done *outside*

the security module (boundary shown as a dashed line in Figure 2), provided that the session key *K* is destroyed reliably after encrypting the data *D* and concealing it via IBE.

2. Roadside system gantry G_2 notices a passing vehicle at (a later) time t. It performs the same steps as G_1 does. In addition, it submits $(t,PK_{2,t})$, along with additional data (vehicle class, road conditions, weather conditions, etc.) as required, to G_1, see message 1 (or vice versa). Alternatively, it is possible to send only the public key along with one additional bit (to indicate which randomizer to use for checking in step 3, see below, within a period of ΔT after switching), so as to avoid sending a timestamp (see later on details).

3. At time $t' > t$, roadside system G_1 receives $(t, PK_{2,t})$ from G_2. Roadside system G_1 filters its list of public keys and selects a set of *n* entries, which are relevant for comparison with $PK_{2,t}$. We denote this (shortened and renamed) list as $\{PK_{1,1}, PK_{1,2}, ..., PK_{1,n}\}$. The check is performed by calculating

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

for all indices $j = 1, 2, ..., n,$ and where y has the same bit-length as the timestamps. The products $PK_{2,t} \cdot PK_{1,j}^{-1} \pmod{p_G}$ can be determined using standard programming libraries for modulo arithmetic and the resulting value *V* is looked up in a pre-computed table.

The pre-computed lookup-table stores pairs (V, time-difference) of the form displayed in Table 1, where ΔT is the time for a travel from G_1 to G_2 at maximal permitted speed for the slowest vehicle class (e.g. 139 seconds for a 5 km distance at speed 130 km/h). Notice that Table 1 can be *pre-computed* and stored as a hash-table (for fast access) in the roadside systems's hardware. Physically impossible values like 0 do not need to be included in the table. Furthermore, for better performance, it is advisable to store more likely time-differences first and unlikely time-differences last when filling the table initially. Alternatively, the hash-table lookup can be replaced by a binary search within a pre-sorted table (at the cost of getting logarithmic running time for the table-lookup).

Table 1: Pre-computed values for speed limit checking

V	Time-Difference
$g^0 \text{MOD} p_g$	0
$g^1 \text{MOD} p_g$	1
$g^2 \text{MOD} p_g$	2
⋮	⋮
$g^{\Delta T} \text{MOD} p_g$	ΔT

For efficiency reasons, G_2 can send $(t, PK_{2,t}^{-1})$ to G_1 and have G_1 compute and look-up $PK_{2,t}^{-1} \cdot PK_{1,j}$ in its table (or vice versa). The contents of Table 1 have to be altered accordingly.

- If the table-lookup comes back negative, i.e. the *value* $V = PK_{2,t} \cdot PK_{1,j}^{-1}$ has not been found, then $x\|y > \Delta T$. This indicates that either $x \neq 0$, so that $LPN_2 \neq LPN_j$, i.e. the license-plate numbers are different, or otherwise $x = 0$ (meaning identical license-plates) and $y = t - t_j > \Delta T$, so that no speed limit violation has happened. In either case, we have no suspect of a violation. In particular, this means that the comparison can practically never yield false-negative alarms.
- If the table-lookup came back positive, then the value $V = g^t(x\|y)$ has been found, and the value x||y can be obtained from the table-lookup ("Time-Difference"-column). Observe that the table may only store records for time-differences up to ΔT. Notice that the randomizers within PK_2 and $PK_{1,j}$ can be assumed identical by virtue of synchronization (cf. below).

  We approximate the likelihood of a false-positive as follows: Let N be the number of entries in Table 1. This value depends on ΔT (e.g. for $\Delta T = 139$ seconds and a time-measurement with an accuracy of 0.01 seconds, we get $N \approx 13900$ entries in the table). The probability for a false-positive is roughly

$$\frac{N}{{}_2 bitlength(p_G)} = \frac{N}{2^{160}} \approx 10^{-44}$$

and thus negligible. So upon a positive table-lookup, we have overwhelmingly strong evidence that the same vehicle has passed both roadside systems within a time shorter than ΔT. This indicates a speed limit violation, which can be passed on to an operator for a manual second check. As far as it regards the automatic checking via the table-lookup, there are practically no false-positive alarms.

4. If a speed limit violation is detected in this way, then G_1 responds to G_2 accordingly, see message 2 in Figure 1 (or vice versa, if the table look-up had been made at G_2), and both send their encrypted evidence data ED_1, ED_2, public keys PK_1, PK_2, encrypted session keys EK_1, EK_2 and the respective roadside system gantry-IDs GID_1, GID_2 to the operator. Messages 3 in Figure 1 (3a and 3b in Figure 3) are sent from G_i to the operator, and are-for $i = 1, 2$ - of the form $(PK_i, EK_i, ED_i, GID_i, H(PK_1 \| PK_2))$, where the last entry $H(PK_1 \| PK_2)$ establishes an optional link between the two messages from both roadside systems. The function H is a cryptographically secure hash-function. The operator can acknowledge both messages by sending a short notification to the roadside systems (to prevent an adversary from blocking this conversation in order to hide a speed limit violation).
The correct response from G_1 to G_2, message 2 (or vice versa) is formed by sending $(PK_2, response)$ with $response \in \{yes,no\}$ to G_2, which assures that G_2 can correctly relate the response to a former query (or vice versa).
5. The operator transmits (PK_1, PK_2) to the key generation center and digitally signs his entire request with his secret signature key $SK_{sig,op}$ (message 4).
6. Upon successful signature verification, the key generation center calculates the decryption keys SK_1, SK_2 referring to PK_1, PK_2. Observe that these decryption keys do neither exist elsewhere in the system nor prior to a suspected speed limit violation. The key generation center encrypts the record (SK_1, SK_2) with the operator's public key PK_{op} and sends an RSA-ciphertext $C = RSA((SK_1, SK_2), PK_{op})$ back to the operator (message 5).
7. The operator decrypts C with his secret key SK_{op} and extracts SK_1, SK_2. These are required to decrypt the session keys EK_1, EK_2 to obtain the AES-keys K_1, K_2, which are used to decrypt the evidence data D_1, D_2. After a manual check for a correctly indicated speed limit violation the evidence data can be forwarded to the legal authorities (message 6).

[0027] Figure 3 displays the whole process as a sequence diagram.

[0028] The process described so far refers to a single vehicle class and optimal road conditions. Depending on the weather conditions and vehicle class, *different* speed limits may apply. This amounts to using a different parameter ΔT when doing the table-lookup upon a request from G_2 (or G_1). There are two basic ways to implement this:

1. Pre-compute Table 1 up to the maximum ΔT of all vehicle classes, and do the look-up to get the actual travel time (or get a "not found" if the travel time was longer than implied by the lowest speed limit on this section). For instance, if a heavy-goods vehicle is limited to 60 km/h (giving $\Delta T_{HGS} = 300\ s$) and a car may drive at up to 130 km/h (giving $\Delta T_{car} = 138\ s$), then the table is computed up to values $g^{\Delta T}$ with $\Delta T = max\{\Delta T_{HGS}, \Delta T_{car}\} = 300\ s$. This determines the size of the table, and the vehicle class (transmitted as additional data in the query) can be used to decide later, whether the speed limit violation has actually occurred, if the look-up came back positive.
2. Alternatively, a different look-up table (Table 1) can be computed specifically for each vehicle class and speed limit. In that case, the transmitted vehicle class determines which table is used for the look-up by RSS. This avoids the additional check required by the single-table approach and is faster because fewer entries have to be searched for each query. Moreover, this hides travel times of vehicles that have been found in the table, but have not committed a speed-limit violation with respect to their specific vehicle class.

[0029] During the system set-up phase, each pair of roadside systems (gantries) can optionally receive a shared randomizer i.e. a random or pseudorandom value. For security, a particular randomizer R_0 should not be shared by more than two roadside systems.

[0030] Particular care has to be taken when changing the randomizer. Let us call the initial randomizer R_0 within both roadside system gantries G_1, G_2 (established during the system initialization). Within e.g. a tamper-proof device (such as a hardware dongle, smartcard, trusted element, cryptoprocessor et cet.), we generate the next randomizer by hashing the last one, i.e. $R_{i+1} = H(R_i)$.

[0031] The randomizer should not leave the tamper-proof device nor be accessible in any way from outside, hence equation (1) should be evaluated within the tamper-proof device. Storing the randomizer externally - if needed - should be done in an encrypted fashion.

[0032] Table 2 in connection with Figure 4 explains which randomizers are used by G_1, G_2 for creating the public keys

("encrypt") and which randomizer is used by G_1 (or G_2) when searching its look-up table upon a request from G_2 (or G_1) ("check").

Table 2: Randomizer Usage for Public-Key Creation and Checking

Arrival time at RSS gantry G_1	**Arrival time at RSS gantry G_2**	
	Before t_{switch}	After t_{switch}
Before t_{switch} - ΔT	Case (a) encrypt G_1:R, encrypt G_2:R check: R	Case (b) encrypt G_1:R, encrypt G_2:R' check: G_1 would check with R' but has deleted the respective public-key by that time, so no speed limit violation has occurred (travel time > ΔT)
Between t_{switch} - ΔT and t_{switch}	Case (c) encrypt G_1:R and R', encrypt G_2:R' check: R	Case (d) encrypt G_1:R and R', encrypt G_2:R' check: R'
After t_{switch}	impossible	Case (e) encrypt G_1:R', encrypt G_2:R' check: R'

[0033] Switching the randomizers is preferably done periodically, provided that the validity period of a randomizer is greater than ΔT in order to avoid synchronization problems. During startup or after a power-failure, G_1 and G_2 could use an authenticated SSL connection to secretly agree on a fresh initial randomizer R_0 and start the hash-chain all over again. This can be done using the standard Station-to-Station protocol such as the Diffie-Hellman Key-exchange. However, this synchronization "from scratch" might only be needed once in a while, e.g. after a power-failure, and is not required to happen very frequently. Alternatively, a manual key-exchange (storage of the new R_0 on a smartcard and copy it from the smartcard into both RSSs) after a power-failure is as well possible. This avoids the need to store designated cryptographic keys for synchronization in each roadside system.

[0034] All traffic from the operator to the KGC can be digitally signed. Notice that it is not required to digitally sign messages 3 from the gantries to the operator, since each roadside system has signed its encrypted evidence data in first instance. This means that no faked evidence data will be accepted for processing by the operator. The respective signature key can be stored in a tamper-proof device. The operator's secret key is protected by a PIN-code to prevent the adversary having compromised the operator's hardware from accessing the key, since the operator's signature key is inaccessible without the PIN.

[0035] The management of SSL-related keys is up to the particular SSL protocol stack implementation. State-of-the-art key-lengths and algorithms can be employed to this end.

[0036] For each component of the system, Table 3 lists the key that it stores, along with the recommended protection for the particular key. The IBE system parameters are assumed authentically known to each component.

Table 3: Overview of cryptographic keys

Component	**Key / Data Item**	**(Cryptographic) Protection**
Roadside System	Secret signature key SK_G	Confidential (inside a tamper-proof device)
Operator	Roadside system's public key(s) PK_G	Authentic (certified)
	Secret signature key $SK_{sig,op}$	Confidential (inside a tamper-proof device, access is PIN-protected
	Secret decryption key SK_{op}	Confidential (same as $SK_{sig,op}$)
Key-Generation Center	Operator's public encryption key PK_{op}	Authentic (certified)
	Operator's public signature verification kev $PK_{sig,op}$	Authentic (certified)

[0037] Table 4 gives a list of system parameters, respective descriptions, owners and visibility of each parameter. For conciseness, we refrain from explicitly listing the specific parameters for each cryptosystem in charge. We propose using RSA and AES to encrypt channels and to use Digital secure standard (DSS) to create digital signatures, although other

encryption and authentication standards known in the art could be used. The respective parameters are implicitly listed in Table 4 through the presence of the respective public and secret keys. All parameters, regardless of their visibility, should be *authentic* at best in order to thwart attacks based on parameter manipulation.

Table 4: System Parameters

Parameter	Semantics and Description	Owner	Visibility
PK_G	Public signature key of each roadside system. Needed to authenticate data submitted to the operator for verification	Roadside system (specific for each gantry)	Public
SK_G	Secret signature creation key of a roadside system. Needed to digitally sign any payload handed over to the operator.	Roadside system (specific for each gantry)	Secret
PK_{op}	Public encryption key of the operator. Used by the KGC to secretly deliver a secret key upon a request.	Operator	Public
SK_{op}	Secret decryption key of the operator. Used to decipher the encrypted secret key for IBE.	Operator	Secret
$PK_{sig,op}$	Public signature key of the operator. Used to verify the authenticity of queries to the KGC.	KGC	Public
$SK_{sig,op}$	Secret signature key of the operator to authenticate queries to the KGC.	Operator	Secret
p_G	A prime number to create encryption keys within a roadside system	Roadside system (same for all cooperating gantries)	Public
g	Generating element of the finite group $Z^{\bullet}_{p_G}$ with modulo multiplication.	Every (cooperating) component in the system	Public
IBE System parameters	See D. Boneh and M. Franklin, *l.c.*	Roadside system (same for all cooperating gantries) and the key-generation center	Public, except for the KGC master-key.

[0038] We recommend the following key-sizes and parameter constraints of Table 5, although not mandatory (*in general,* we say that a number n has bit-length t if $2^{t-1} \leq n < 2^t$).

Table 5: Recommended Key Sizes (Security parameter t)

Cryptosystem	Parameter constraints
RSA encryption	Primes p, q of minimum bit-length t = 2048 Bit (NIST recommendation)
DSA Digital Signatures	Primes p, q where p has minimal bit-length t = 1024 Bit and q has minimal bit-length t = 160 Bit
Identity Based Encryption	Prime q with bit-length at least t = 160 Bit
Finite group $Z^{\bullet}_{p_G}$	Prime p_G with bit-length at least t = 160 Bit

[0039] As far as identity based encryption (IBE) is concerned, apart from the above recommended key-sizes no other constraints on the curves (such as minimal class number or others) used for digital signatures apply since we deal with encryption and not with signatures of the Boneh-Franklin scheme. Nevertheless, we recommend the key-sizes used for signatures to be used as well for IBE.

[0040] In general, it is advisable to ensure that the discrete logarithm or factorization problem in the group that we are using is hard. The *bit-strength b* measures the efforts of factorizing an integer or finding a discrete logarithm, compared

to a brute-force search over a set of 2^b values. Hence, an example interpretation of Table 6 is the following: The last row in the table tells that finding a discrete logarithm modulo a prime of at least 256 Bit size (using Pollard's rhoalgorithm, cf. A. Menezes, P.C. van Oorschot and S. Vanstone: Handbook of applied Cryptography, CRC Press LLC, 1997) is equally difficult as brute-force breaking trying all 2^{128} keys to a symmetric cipher, or equivalently hard as factoring an integer with 3072 Bit. Comparing the values in Table 5 to the recommendations given by Table 6, we recommend the latter sizes for security, since these agree with standardized recommendations, yet provide better long-term security:

Table 6: Equivalent cryptographic strength provided by different algorithms

Bit-strength	Size of group (prime)	Size of Integer or Finite Field
80	160	1024
112	224	2048
128	256	3072
192	384	7168
256	512	15360

Claims

1. A method for detecting a speed violation of a vehicle traveling from a first roadside system (G_1) to a second roadside system (G_2), comprising:

   setting-up private and public parameters (g, p_G), including a common modulo basis (p_G), of an identity based encryption IBE scheme in a key generation center *(KGC)* and the first and second roadside systems (G_1, G_2);
   capturing at least an identifier (*LPN*) of the vehicle and a first timestamp (t) at the first roadside system (G_1) as first evidence data (D), using at least the first identifier (*LPN*) and first timestamp (t) as a first identity to generate a first IBE public key ($PK_{1,t}$), encrypting the first evidence data (D) with a first random session key (K), encrypting the first random session key (K) with the first IBE public key ($PK_{1,t}$), and deleting the first evidence data (D) and the first random session key (K) at the first roadside system (G_1);
   capturing at least an identifier (*LPN*) of the vehicle and a second timestamp (t) at the second roadside system (G_2) as second evidence data (D), using at least the second identifier (*LPN*) and second timestamp (t) as a second identity to generate a second IBE public key ($PK_{2,t}$), encrypting the second evidence data (D) with a second random session key (K), encrypting the second random session key (K) with the second IBE public key ($PK_{2,t}$), and deleting the second evidence data (D) and the second random session key *(K)* at the second roadside system (G_2);
   calculating a ratio (V) of the first and second public keys ($PK_{1,t}$, $PK_{2,t}$), modulo the common modulo basis (p_G), and looking-up the ratio (V) in a table of ratios (V) pre-computed for a set of time differences between said first and second timestamps (t) which set represents speed violations, and, when the look-up is successful:

      retrieving at least one IBE private key (SK_1, SK_2) for at least one of said IBE public keys ($PK_{1,t}$, $PK_{2,t}$) from the key generation center (*KGC*), decrypting at least one of said encrypted session keys (*EK*) with said private key (SK_1, Sk_2), and decrypting at least one of said encrypted evidence data (*ED*) with said decrypted session key (K).

2. The method of claim 1, wherein the IBE scheme is a Boneh-Franklin encryption scheme.

3. The method of claim 1 or 2, wherein the evidence data (D) is encrypted with the session key (K) according to a symmetric encryption scheme.

4. The method of claim 3, wherein the symmetric encryption scheme is the advanced encryption standard (AES).

5. The method of any of the claims 1 to 4, wherein the first and second roadside systems (G_1, G_2) share at least one random or pseudorandom value (R_i) which is incorporated into the first identity to generate the first IBE public key ($PK_{1,t}$) and into the second identity to generate the second IBE public key ($PK_{2,t}$).

6. The method of claim 5, wherein the first IBE public key ($PK_{1,t}$) is generated in the form

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

with

$PK_{1,t}$ being the first IBE public key,
LPN, t being the identifier and timestamp of the first evidence data,
R_i being the random or pseudorandom value,
g, p_G being public parameters of the IBE scheme,

and the second IBE public key is generated in the form

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

with

$PK_{2,t}$ being the second IBE public key,
LPN, t being the identifier and timestamp of the second evidence data,
R_i being the random or pseudorandom value, and
g, p_G being public parameters of the IBE scheme.

7. The method of claim 6, wherein the ratio (V) is calculated in the form

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

8. The method of any of the claims 5 to 7, wherein the first and second roadside systems (G_1, G_2) communicate to synchronously switch from one pseudorandom value (R_i) to a subsequent pseudorandom value (R_i) in a series of pseudorandom values (R_i).

9. The method of any of the claims 1 to 8, wherein the first evidence data (D) comprises a picture (PIC) of the vehicle taken with a camera at the first roadside system (G_1), and the second evidence data (D) comprises a picture (PIC) of the vehicle taken with a camera at the second roadside system (G_2).

10. The method of any of the claims 1 to 9, wherein the first evidence data (D) is cryptographically signed with a signature key (SK_G) of the first roadside system (G_1), and the second evidence data (D) is cryptographically signed with a signature key (SK_G) of the second roadside system (G_2).

11. The method of any of the claims 1 to 10, wherein the session key (K) has at least 128 bits.

12. The method of any of the claims 1 to 11, wherein the first and second IBE public keys ($PK_{1,t}$, $PK_{2,t}$), the encrypted first and second session keys (EK) and the encrypted first and second evidence data (ED) are deleted after a predetermined period of time (ΔT).

13. The method of any of the claims 1 to 12, wherein the first evidence data (D) comprises a class (VC) of the vehicle captured at the first roadside system (G_1).

14. The method of claim 13, wherein different tables of ratios (V) are pre-computed for different classes (VC) of vehicles and the table used for the look-up is chosen according to the captured class of the vehicle.

15. The method of any of the claims 1 to 14, wherein the first or second evidence data (D) comprises a weather or road condition (AD) captured at the first or second roadside system (G_1, G_2), and wherein different tables of ratios (V) are pre-computed for different conditions and the table used for the look-up is chosen according to the captured condition.

16. The method of any of the claims 1 to 15, wherein the first IBE public key ($PK_{1,t}$) is sent to the second roadside system (G_2) or the second IBE public key ($PK_{2,t}$) is sent to the first roadside system (G_1) for calculating the ratio (V).

Patentansprüche

1. Verfahren zum Detektieren einer Geschwindigkeitsübertretung eines Fahrzeugs, das von einem ersten straßenseitigen System (G_1) zu einem zweiten straßenseitigen System (G_2) fährt, umfassend:

Erstellen von privaten und öffentlichen Parametern (g, p_G), mit einer gemeinsamen Modulo-Basis (p_G), eines identitätsbasierten Verschlüsselungsschemas IBE in einer Schlüsselgenerierungszentrale (KGC) und dem ersten und dem zweiten straßenseitigen System (G_1, G_2);
Erfassen zumindest eines Identifikators (LPN) des Fahrzeugs und eines ersten Zeitstempels (t) am ersten straßenseitigen System (G_1) als erste Beweisdaten (D), Verwenden zumindest des ersten Identifikators (LPN) und ersten Zeitstempels (t) als erste Identität, um einen ersten öffentlichen IBE-Schlüssel ($PK_{1,t}$) zu erzeugen, Verschlüsseln der ersten Beweisdaten (D) mit einem ersten zufälligen Sitzungsschlüssel (K), Verschlüsseln des ersten zufälligen Sitzungsschlüssels (K) mit dem ersten öffentlichen IBE-Schlüssel ($PK_{1,t}$), und Löschen der ersten Beweisdaten (D) and des ersten zufälligen Sitzungsschlüssels (K) am ersten straßenseitigen System (G_1);
Erfassen zumindest eines Identifikators (LPN) des Fahrzeugs und eines zweiten Zeitstempels (t) am zweiten straßenseitigen System (G_2) als zweite Beweisdaten (D), Verwenden zumindest des zweiten Identifikators (LPN) und zweiten Zeitstempels (t) als zweite Identität, um einen zweiten öffentlichen IBE-Schlüssel ($PK_{2,t}$) zu erzeugen, Verschlüsseln der zweiten Beweisdaten (D) mit dem zweiten öffentlichen IBE-Schlüssel ($PK_{2,t}$), und Löschen der zweiten Beweisdaten (D) und des zweiten zufälligen Sitzungsschlüssels (K) am zweiten straßenseitigen System (G_2);
Berechnen eines Verhältnisses (V) des ersten und des zweiten öffentlichen Schlüssels ($PK_{1,t}$, $PK_{2,t}$), modulo der gemeinsamen Modulo-Basis (p_G), und Nachschlagen des Verhältnisses (V) in einer vorberechneten Tabelle von Verhältnissen (V) für einen Satz von Zeitdifferenzen zwischen dem ersten und dem zweiten Zeitstempel (t), wobei der Satz Geschwindigkeitsüberschreitungen repräsentiert, und, wenn das Nachschlagen erfolgreich ist:

Abrufen zumindest eines privaten IBE-Schlüssels (SK_1, SK_2) für zumindest einen der genannten öffentlichen IBE-Schlüssel ($PK_{1,t}$, $PK_{2,t}$) von der Schlüsselgenerierungszentrale (KGC), Entschlüsseln zumindest eines der genannten verschlüsselten Sitzungsschlüssel (EK) mit dem genannten privaten Schlüssel (SK_1, SK_2), und Entschlüsseln zumindest einer der genannten verschlüsselten Beweisdaten (ED) mit dem genannten entschlüsselten Sitzungsschlüssel (K).

2. Verfahren nach Anspruch 1, wobei das IBE-Schema ein Boneh-Franklin-Verschlüsselungsschema ist.

3. Verfahren nach Anspruch 1 oder 2, wobei die Beweisdaten (D) mit dem Sitzungsschlüssel (K) nach einem symmetrischen Verschlüsselungsschema verschlüsselt werden.

4. Verfahren nach Anspruch 3, wobei das symmetrische Verschlüsselungsschema der Advanced Encryption Standard (AES) ist.

5. Verfahren nach einem der Ansprüche 1 bis 4, wobei das erste und das zweite straßenseitige System (G_1, G_2) zumindest einen zufälligen oder pseudozufälligen Wert (R_i) gemein haben, der in die erste Identität integriert wird, um den ersten öffentlichen IBE-Schlüssel ($PK_{1,t}$) zu generieren, und in die zweite Identität, um den zweiten öffentlichen IBE-Schlüssel ($PK_{2,t}$) zu generieren.

6. Das Verfahren nach Anspruch 5, wobei der erste öffentliche IBE-Schlüssel ($PK_{1,t}$) in der Form

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

generiert wird, wobei

$PK_{1,t}$ der erste öffentliche IBE-Schlüssel ist,
LPN, t der Identifikator und Zeitstempel der ersten Beweisdaten sind,
R_i der zufällige oder pseudozufällige Wert ist, und
g, p_G öffentliche Parameter des IBE-Schemas sind,

und der zweite öffentliche IBE-Schlüssel in der Form

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

generiert wird, wobei

$PK_{2,t}$ der zweite öffentliche IBE-Schlüssel ist,
LPN, t der Identifikator und Zeitstempel der zweiten Beweisdaten sind,
R_i der zufällige oder pseudozufällige Wert ist, und
g, p_G öffentliche Parameter des IBE-Schemas sind.

7. Verfahren nach Anspruch 6, wobei das Verhältnis (V) in der Form

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

berechnet wird.

8. Verfahren nach einem der Ansprüche 5 bis 7, wobei das erste und das zweite straßenseitige System (G_1, G_2) kommunizieren, um synchron von einem pseudozufälligen Wert (R_i) zu einem darauffolgenden pseudozufälligen Wert (R_i) in einer Reihe von pseudozufälligen Werten (R_i) zu wechseln.

9. Verfahren nach einem der Ansprüche 1 bis 8, wobei die ersten Beweisdaten (D) ein Bild (PIC) des Fahrzeugs umfassen, das mit einer Kamera bei dem ersten straßenseitigen System (G_1) aufgezeichnet wurde, und die zweiten Beweisdaten (D) ein Bild (PIC) des Fahrzeugs umfassen, das mit einer Kamera bei dem zweiten straßenseitigen System (G_1) aufgezeichnet wurde.

10. Verfahren einer der Ansprüche 1 bis 9, wobei die ersten Beweisdaten (D) mit einem Signaturschlüssel (SK_G) des ersten straßenseitigen Systems (G_1) kryptographisch signiert werden, und die zweiten Beweisdaten (D) mit einem Signaturschlüssel (SK_G) des zweiten straßenseitigen Systems (G_2) kryptographisch signiert werden.

11. Verfahren nach einem der Ansprüche 1 bis 10, wobei der Sitzungsschlüssel (K) zumindest 128 Bit hat.

12. Verfahren nach einem der Ansprüche 1 bis 11, wobei der erste und zweite öffentliche IBE-Schlüssel ($PK_{1,t}$, $PK_{2,t}$), der verschlüsselte erste und zweite Sitzungsschlüssel (EK) und die verschlüsselten ersten und zweiten Beweisdaten (ED) nach einem vorbestimmten Zeitintervall (ΔT) gelöscht werden.

13. Verfahren nach einem der Ansprüche 1 bis 12, wobei die ersten Beweisdaten (D) eine Klasse (VC) des vom ersten straßenseitigen Systems (G_1) erfassten Fahrzeugs umfassen.

14. Das Verfahren nach Anspruch 13, wobei verschiedene Tabellen von Verhältnissen (V) für verschiedene Klassen (VC) von Fahrzeugen vorberechnet werden und die für das Nachschlagen verwendete Tabelle nach der erfassten Klasse des Fahrzeugs ausgewählt wird.

15. Verfahren nach einem der Ansprüche 1 bis 14, wobei die ersten oder zweiten Beweisdaten (D) einen bei dem ersten oder zweiten straßenseitigen System (G_1, G_2) erfassten Wetter- oder Straßenzustand (AD) umfassen und wobei verschiedene Tabellen von Verhältnissen (V) für verschiedene Zustände vorberechnet werden und die für das Nachschlagen verwendete Tabelle nach dem erfassten Zustand ausgewählt wird.

16. Verfahren nach einem der Ansprüche 1 bis 15, wobei der erste öffentliche IBE-Schlüssel ($PK_{1,t}$) an das zweite

straßenseitige System (G_2) oder der zweite öffentliche IBE-Schlüssel ($PK_{2,t}$) an das erste straßenseitige System (G_1) gesendet wird, um das Verhältnis (V) zu berechnen.

Revendications

1. Procédé pour la détection d'un excès de vitesse d'un véhicule circulant d'un premier système de bord de route (G_1) à un deuxième système de bord de route *(G_2),* comprenant :

   la mise en place de paramètres privés et publics (g, p_G), y compris une base modulo commune (p_G), d'un schéma de cryptage basé sur l'identité IBE dans un centre de génération de clés (*KGC*) et les premier et deuxième systèmes de bord de route (G_1, G_2);
   la saisie d'au moins un identifiant (*LPN*) du véhicule et d'un premier horodatage (*t*) au niveau du premier système de bord de route (G_1) en tant que premières données de preuve (*D*), à l'aide au moins du premier identifiant (*LPN*) et du premier horodatage (*t*) en tant que première identité pour générer une première clé publique IBE ($PK_{1,t}$), cryptant les premières données de preuve (*D*) avec une première clé de session aléatoire (*K*), cryptant la première clé de session aléatoire (*K*) avec la première clé publique IBE ($PK_{1,t}$), et supprimant les premières données de preuve (*D*) et la première clé de session aléatoire (*K*) au niveau du premier système de bord de route (G_1) ;
   la saisie d'au moins un identifiant (*LPN*) du véhicule et d'un deuxième horodatage (t) au niveau du deuxième système de bord de route (G_2) en tant que deuxièmes données de preuve (*D*), à l'aide au moins du deuxième identifiant (*LPN*) et du deuxième horodatage (*t*) en tant que deuxième identité pour générer une deuxième clé publique IBE ($PK_{2,t}$), cryptant les deuxièmes données de preuve (*D*) avec une deuxième clé de session aléatoire (*K*), cryptant la deuxième clé de session aléatoire (*K*) avec la deuxième clé publique IBE ($PK_{2,t}$), et supprimant les deuxièmes données de preuve (*D*) et la deuxième clé de session aléatoire (*K*) au niveau du deuxième système de bord de route (G_2) ;
   le calcul d'un ratio (*V*) des première et deuxième clés publiques ($PK_{1,t}$; $PK_{2,t}$), modulo la base modulo commune (p_G), et la recherche du ratio (*V*) dans un tableau de ratios (*V*) précalculés pour un ensemble de différences temporelles entre lesdits premier et deuxième horodatages (*t*), ledit ensemble représentant des excès de vitesse, et, lorsque la recherche a réussi :

      récupération d'au moins une clé privée IBE (*SK1, SK2*) pour au moins l'une desdites clés publiques IBE ($PK_{1,t}$; $PK_{2,t}$) du centre de génération de clés (*KGC*), décryptage d'au moins l'une desdites clés de session cryptées (*EK*) avec ladite clé privée (*SK1*, *SK2),* et décryptage d'au moins l'une desdites données de preuve cryptées (*ED*) avec ladite clé de session décryptée (*K*).

2. Procédé selon la revendication 1, dans lequel le schéma IBE est un schéma de cryptage Boneh-Franklin.

3. Procédé selon la revendication 1 ou 2, dans lequel les données de preuve (*D*) sont cryptées avec la clé de session (*K*) selon un schéma de cryptage symétrique.

4. Procédé selon la revendication 3, dans lequel le schéma de cryptage symétrique est l'Advanced Encryption Standard (AES).

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel les premier et deuxième systèmes de bord de route (G_1, G_2) partagent au moins une valeur aléatoire ou pseudo-aléatoire (R_i) incorporée dans la première identité pour générer la première clé publique IBE ($PK_{1,t}$) et dans la deuxième identité pour générer la deuxième clé publique IBE ($PK_{2,t}$).

6. Procédé selon la revendication 5, dans lequel la première clé publique IBE ($PK_{1,t}$) est générée sous la forme

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

où

$PK_{1,t}$ correspond à la première clé publique IBE,

LPN, t correspondent à l'identifiant et à l'horodatage des premières données de preuve,
R_i correspond à la valeur aléatoire ou pseudo-aléatoire,
g, P_G correspondent aux paramètres publics du modèle IBE,

et la deuxième clé publique IBE est générée sous la forme

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

où

$PK_{2,t}$ correspond à la deuxième clé publique IBE,
LPN, t correspondent à l'identifiant et à l'horodatage des deuxièmes données de preuve,
R_i correspond à la valeur aléatoire ou pseudo-aléatoire, et
g, P_G correspondent aux paramètres publics du modèle IBE.

7. Procédé selon la revendication 6, dans lequel le ratio (*V*) est calculé sous la forme

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

8. Procédé selon l'une quelconque des revendications 5 à 7, dans lequel les premier et deuxième systèmes de bord de route (G_2) communiquent pour commuter de façon synchrone d'une valeur pseudo-aléatoire (R_i) à une valeur pseudo-aléatoire (R_i) suivante dans une série de valeurs pseudo-aléatoires (R_i).

9. Procédé selon l'une quelconque des revendications 1 à 8, dans lequel les premières données de preuve (*D*) comprennent une image (*PIC*) du véhicule prise avec une caméra au niveau du premier système de bord de route (G_1), et les deuxièmes données de preuve (*D*) comprennent une image (*PIC*) du véhicule prise avec une caméra au niveau du deuxième système de bord de route (G_2).

10. Procédé selon l'une quelconque des revendications 1 à 9, dans lequel les premières données de preuve (*D*) sont signées de façon cryptographique avec une clé de signature (SK_G) du premier système de bord de route (G_1), et les deuxièmes données de preuve (*D*) sont signées de façon cryptographique avec une clé de signature (SK_G) du deuxième système de bord de route (G_2).

11. Procédé selon l'une quelconque des revendications 1 à 10, dans lequel la clé de session (*K*) a au moins 128 bits.

12. Procédé selon l'une quelconque des revendications 1 à 11, dans lequel les première et deuxième clés publiques IBE ($PK_{1,t}$, $PK_{2,t}$), les première et deuxième clés de session cryptées (*EK*) et les premières et deuxièmes données de preuve (*ED*) sont effacées après une période de temps prédéterminée (ΔT).

13. Procédé selon l'une quelconque des revendications 1 à 12, dans lequel les premières données de preuve (*D*) comprennent une classe (*VC*) du véhicule, saisie au niveau du premier système de bord de route (G_1).

14. Procédé selon la revendication 13, dans lequel les différents tableaux de ratios (*V*) sont précalculés pour différentes classes (*VC*) de véhicules, et le tableau utilisé pour la recherche est choisi en fonction de la classe de véhicule saisie.

15. Procédé selon l'une quelconque des revendications 1 à 14, dans lequel les premières et deuxièmes données de preuve (*D*) comprennent une condition météorologique ou routière (*AD*) saisie au niveau du premier ou du deuxième système de bord de route (G_1, G_2), et dans lequel différents tableaux de ratios (*V*) sont précalculés pour différentes conditions, et le tableau utilisé pour la recherche est choisi en fonction de la condition saisie.

16. Procédé selon l'une quelconque des revendications 1 à 15, dans lequel la première clé publique IBE ($PK_{1,t}$) est envoyée au deuxième système de bord de route (G_2) ou la deuxième clé publique IBE ($PK_{2,t}$) est envoyée au premier système de bord de route (G_1) pour le calcul du ratio (*V*).

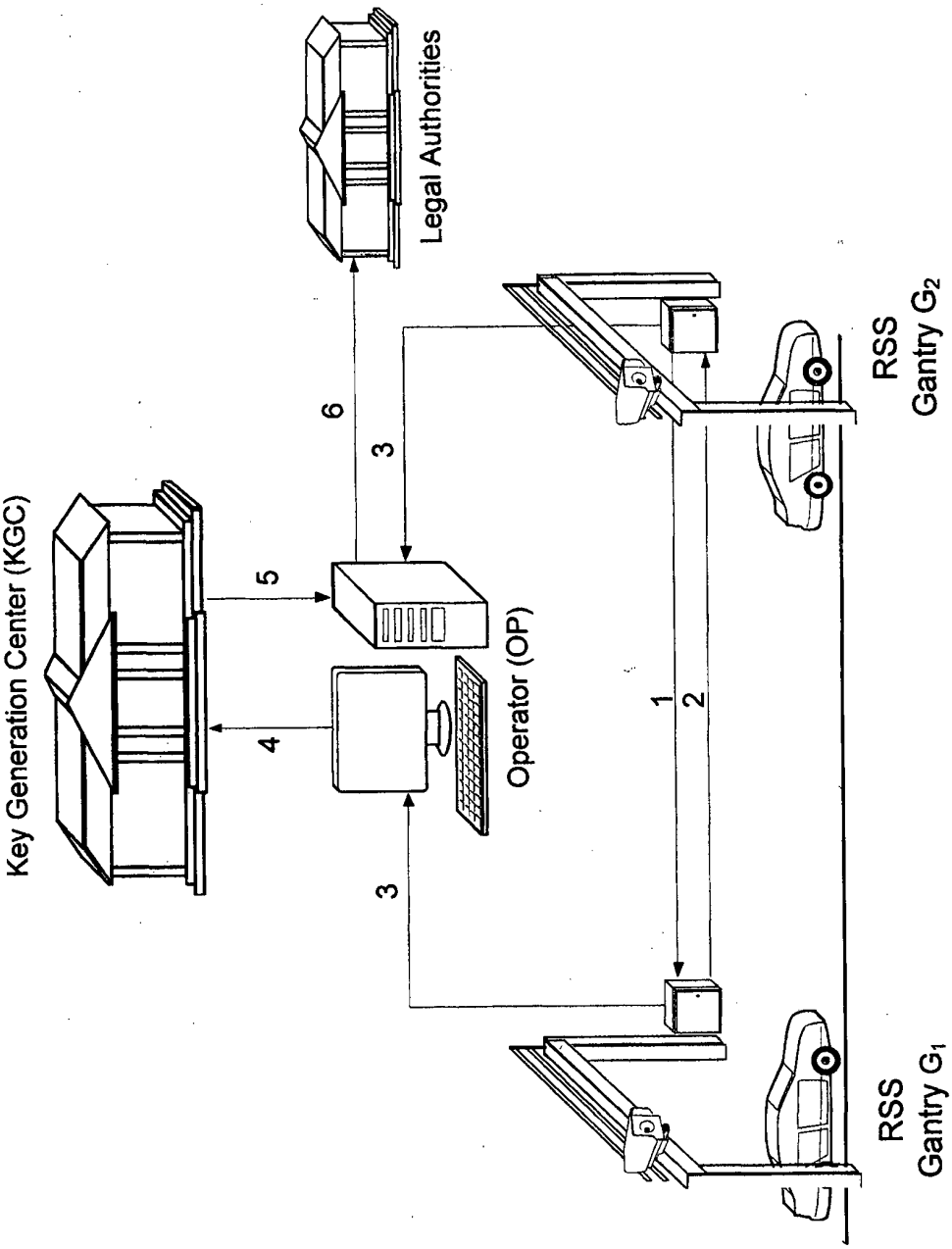
Legal Authorities
Key Generation Center (KGC)
Operator (OP)
RSS
Gantry G_2
RSS
Gantry G_1
1
2
3
3
3
4
5
6

Fig. 1

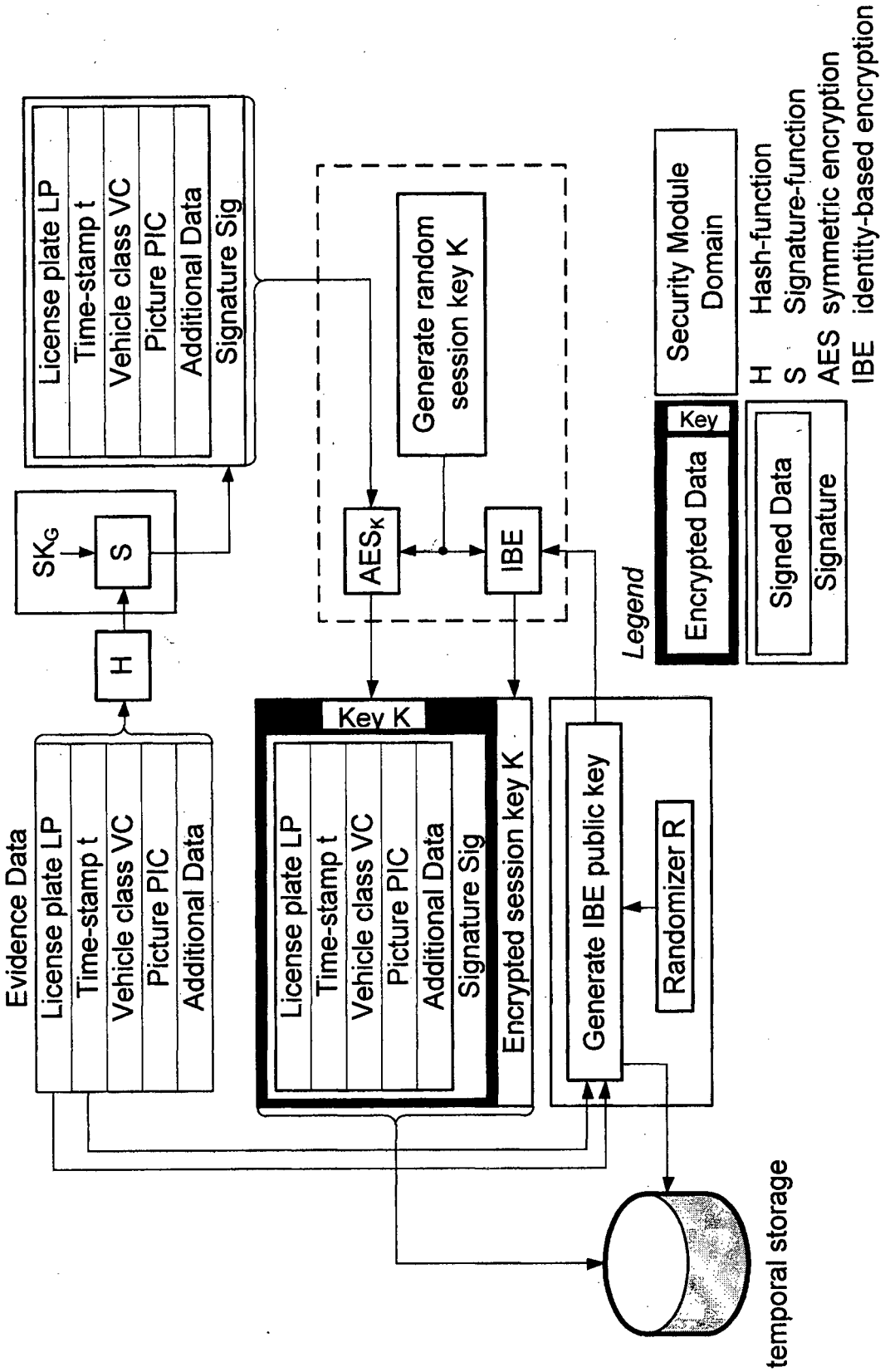
Evidence Data
License plate LP
Time-stamp t
Vehicle class VC
Picture PIC
Additional Data
H
SKG
S
License plate LP
Time-stamp t
Vehicle class VC
Picture PIC
Additional Data
Signature Sig
Generate random session key K
AESK
IBE
Key K
License plate LP
Time-stamp t
Vehicle class VC
Picture PIC
Additional Data
Signature Sig
Encrypted session key K
Generate IBE public key
Randomizer R
temporal storage
Legend
Security Module Domain
Key
Encrypted Data
Signed Data
Signature
H Hash-function
S Signature-function
AES symmetric encryption
IBE identity-based encryption

Fig. 2

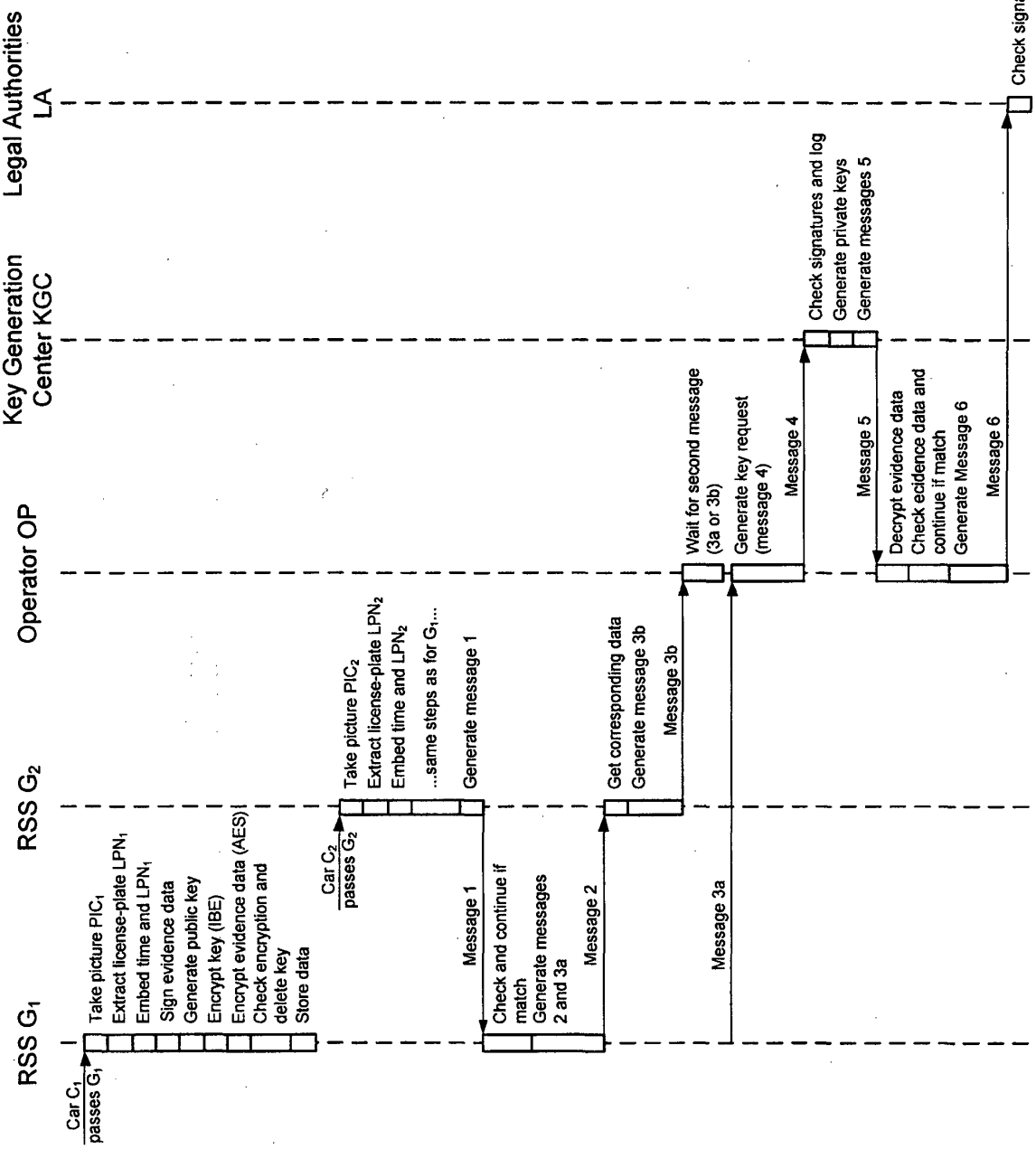
RSS G1
RSS G2
Operator OP
Key Generation Center KGC
Legal Authorities LA
Car C1 passes G1
Take picture PIC1
Extract license-plate LPN1
Embed time and LPN1
Sign evidence data
Generate public key
Encrypt key (IBE)
Encrypt evidence data (AES)
Check encryption and delete key
Store data
Car C2 passes G2
Take picture PIC2
Extract license-plate LPN2
Embed time and LPN2
...same steps as for G1...
Generate message 1
Message 1
Check and continue if match
Generate messages 2 and 3a
Message 2
Get corresponding data
Generate message 3b
Message 3b
Message 3a
Wait for second message (3a or 3b)
Generate key request (message 4)
Message 4
Check signatures and log
Generate private keys
Generate messages 5
Message 5
Decrypt evidence data
Check ecidence data and continue if match
Generate Message 6
Message 6
Check signatures and log

Fig. 3

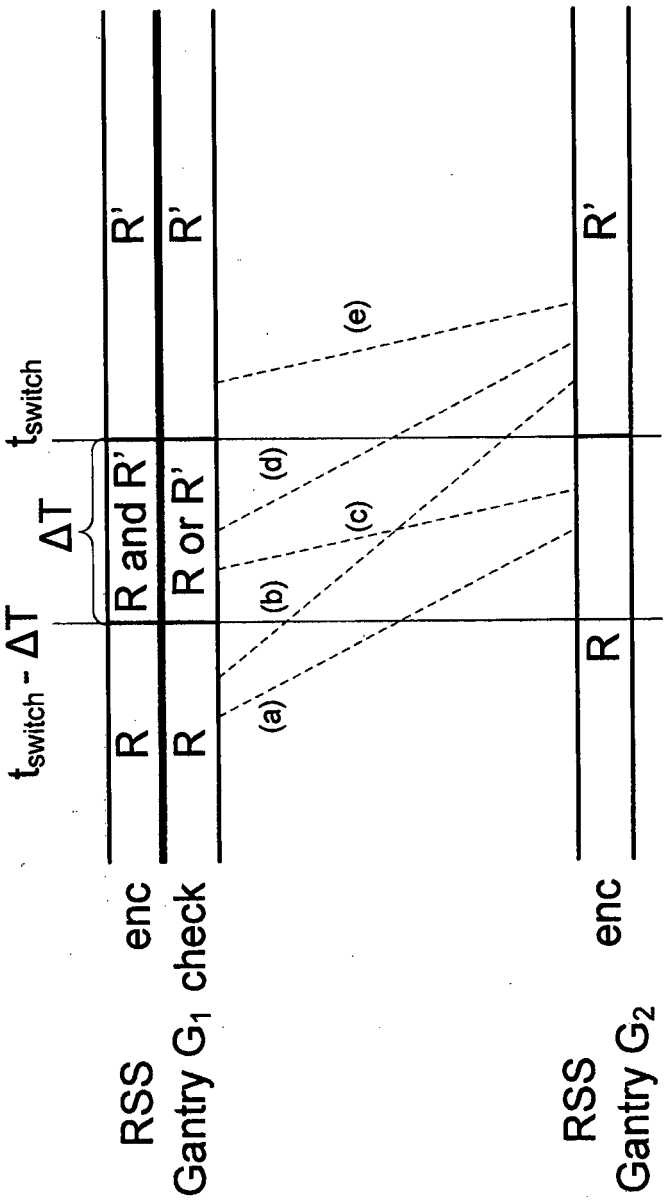
RSS
Gantry G1
enc
check
R
R
R and R'
R or R'
R'
R'
(a)
(b)
(c)
(d)
(e)
tswitch - ΔT
ΔT
tswitch
RSS
Gantry G2
enc
R
R'

Fig. 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 2220634 A **[0004]**
- EP 2360647 A **[0004]**

Non-patent literature cited in the description

- **D. BONEH ; M. FRANKLIN.** Identity based encryption from the Weil pairing. *SIAM J. of Computing,* 2003, vol. 32, 586-615 **[0026]**
- **L. MARTIN.** Introduction to Identity-Based Encryption. Artech House, 2008 **[0026]**
- **A. MENEZES ; P.C. VAN OORSCHOT ; S. VANSTONE.** Handbook of applied Cryptography. CRC Press LLC, 1997 **[0040]**