Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

Int.Cl.: G 08 G 1/054 (2006.01) H 04 L 9/08 (2006.01) H 04 L 29/06 (2006.01)

Oversættelsen bekendtgjort den: 2015-02-23


Europæisk ansøgning nr.: 12455003.9

Europæisk indleveringsdag: 2012-04-06

Den europæiske ansøgnings publiceringsdag: 2013-10-09

Designerede stater: 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

Patenthaver: Kapsch TrafficCom AG, Am Europaplatz 2, 1120 Wien, Østrig

Oplifter: Abl, Alexander, Tiroler Weg 6/2, 9073 Viktring, Østrig
Rass, Stefan, Hans-Sachs Strasse 23/10, 9020 Klagenfurt, Østrig
Schartner, Peter, Kranzmayerstrasse 61A, 9020 Klagenfurt, Østrig
Horster, Patrick, Schervierstrasse 19, 50226 Frechen, Tyskland

Fuldmandig i Danmark: Dennemeyer & Associates S.A, Bavariastr. 7, D-80336 München, Tyskland

Benævnelse: FREMGANGSMÅDE TIL DETEKTERING AF ET KØRETØJS HASTIGHEDSOVERTRÆDELSE

Fremdragne publikationer:
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-
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 roadside 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.

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 driver's 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.

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

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.

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.

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

\[ PK_{1,t} := g^{(LPN \mid t) \oplus R_1} \mod p_G \]

with

- \( PK_{1,t} \) being the first IBE public key,
- \( LPN, t \) being the identifier and timestamp of the first evidence data,
- \( R_1 \) 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

\[ PK_{2,t} := g^{(LPN \mid t) \oplus R_2} \mod p_G \]

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
$g_{\rho_G}$ being public parameters of the IBE scheme;

and the ratio is preferably calculated in the form

$$PK_{2j} \cdot PK_{1j} \cdot (\mod \rho_G)$$

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

- The face of the driver (insular legal regulations permit this).
- A unique identification token of the roadside system where the picture has been taken (i.e. a proof of origin.
of the picture).
- The license-plate number as vehicle identifier.
- The current traffic and weather conditions, including the position and lane of all relevant vehicles.
- A vehicle class detector.
- 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.

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).

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 G₁, G₂, 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 cryptocontroller) 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.

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 G₁.

1. The roadside system at gantry G₁ 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 G₁ and G₂. This respective information is assumed available to both gantries, G₁ and G₂.

   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 \( SK_{G1} \) 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 \( PK_{G1} \) 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
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 $PK_{t,j}$ of the IBE scheme is created (e.g. within a tamper-proof device) as:

$$PK_{t,j} = g^{([LPN\parallel pad)\oplus R_j]\parallel l} \mod p_G$$

(1)

where $\parallel$ 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 BE 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.

- $R_j$ 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 $R_j$ with the license-plate number (and padding) thwart 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 $PK_{t,j}$, the first roadside system of a section pair encrypts the session key to obtain $EK = IBE(K, PK_{t,j})$.

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 $PK_{t,j}$ 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 $\Delta T$ 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 $\Delta T$): 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

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

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 $\Delta T$. A key can be stored along with the time of its creation, i.e. a record can be e.g. of the form $(PK_{t,j})$.

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 G₂ notices a passing vehicle at (a later) time t. It performs the same steps as G₁ does. In addition, it submits \((LPK_{2,0})\), along with additional data (vehicle class, road conditions, weather conditions, etc.) as required, to G₁, 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 \(\Delta T\) after switching), so as to avoid sending a timestamp (see later on details).

3. At time \(t' > t\), roadside system G₁ receives \((t, PK_{2,t'})\) from G₂. Roadside system G₁ 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 \(\{PK_{1,t}, PK_{1,t}, ..., PK_{1,t}\}\). The check is performed by calculating

\[
V = PK_{2,t'} \cdot PK_{1,t}^{-1} \pmod{p_G} \\
= g^{(LPW_{1,t} \cdot \Delta t)} \cdot g^{(LPW_{2,t} \cdot \Delta t)} \pmod{p_G} \\
= g^{x \cdot y} \pmod{p_G} 
\]

for all indices \(j = 1, 2, ..., n\), and where \(y\) has the same bit-length as the timestamps. The products \(PK_{2,t'} \cdot PK_{1,t}^{-1} \pmod{p_G}\) 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 \((V, t' - t)\) of the form displayed in Table 1, where \(\Delta T\) is the time for a travel from G₂ to G₁ at maximal permitted speeds 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

<table>
<thead>
<tr>
<th>V</th>
<th>Time-Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>(g^{\ast MODP_{p_G}})</td>
<td>0</td>
</tr>
<tr>
<td>(g^{\ast MODP_{p_G}})</td>
<td>1</td>
</tr>
<tr>
<td>(g^{2 \ast MODP_{p_G}})</td>
<td>2</td>
</tr>
<tr>
<td>(\ast )</td>
<td>(\Delta T)</td>
</tr>
<tr>
<td>(g^{\ast T \ast MODP_{p_G}})</td>
<td>(\Delta T)</td>
</tr>
</tbody>
</table>

For efficiency reasons, G₂ can send \((t, PK_{2,t'})\) to G₁ and have G₁ compute and look-up \(PK_{2,t'} \cdot PK_{1,t}\) 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 \(V = PK_{2,t'} \cdot PK_{1,t}^{-1}\) has not been found, then \(x \cdot y > \Delta T\). This indicates that either \(x = 0\), so that \(LPW_{2} \neq LPW_{1}\) i.e. the license-plate numbers are different, or otherwise \(x = 0\) (meaning identical license-plates) and \(y = t' - t > \Delta T\), 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 \(V = g^{x \cdot y}\) has been found, and the value \(x \cdot y\) can be obtained from the table-lookup ("Time-Difference"-column). Observe that the table may only store records for time-differences up to \(\Delta T\). Notice that the randomizers within \(PK_{2}\) and \(PK_{1}\) 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 \(\Delta T\) (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
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 \( \Delta T \). 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 \( G_1 \) to the operator, and are of the form \( (PK_1, EK_1, ED_1, GID_1, H(PK_2)) \), whereas the last entry \( H(PK_2) \) 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 \( (PK_2, \text{response \ e \ (yes,no)} \) to \( G_2 \), which assures that \( G_2 \) can correctly relate the response to a former query (or vice versa).

5. The operator transmits \( (PK_2, PK_2) \) to the key generation center and digitally signs his entire request with his secret signature key \( SK_{sig} \) (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 not exist elsewhere in the system nor prior to a suspected speed limit violation. The key generation center decrypts the record \( (SK_1, SK_2) \) with the operator's public key \( PK_{op} \) and sends an RSA-ciphertext \( C = RSA(\langle SK_1, SK_2, PK_{op} \rangle) \) back to the operator (message 5).

7. The operator decrypts \( C \) with his secret key \( SK_{op} \) and obtains \( SK_1, SK_2 \). 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).

The process described so far refers to a single vehicle class and optional road conditions. Depending on the weather conditions and vehicle class, different speed limits may apply. This amounts to using a different parameter \( \Delta T \) 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 \( \Delta T \) 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 \( \Delta T_{car} = 130 \) s), then the table is computed up to values \( \Delta T \) 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.

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.

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 etc.), we generate the next randomizer by hashing the last one, i.e. \( R_{n+1} = H(R_0) \).

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.

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>
<thead>
<tr>
<th>Arrival time at RSS gantry (G_1)</th>
<th>Arrival time at RSS gantry (G_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before (t_{\text{switch}}) (-\Delta T)</td>
<td>Before (t_{\text{switch}}) (-\Delta T)</td>
</tr>
<tr>
<td>Case (a) encrypt (G_1;R), encrypt (G_2;R)</td>
<td>Case (b) encrypt (G_2;R), encrypt (G_2;R') check: (G_2) would check with (R) but has deleted the respective public-key by that time, so no speed limit violation has occurred (travel time (&gt;\Delta T))</td>
</tr>
<tr>
<td>Before (t_{\text{switch}}) (-\Delta T) and (t_{\text{switch}})</td>
<td>Between (t_{\text{switch}}) (-\Delta T) and (t_{\text{switch}})</td>
</tr>
<tr>
<td>Case (c) encrypt (G_1;R) and (R'), encrypt (G_2;R') check: (R)</td>
<td>Case (d) encrypt (G_1;R) and (R'), encrypt (G_2;R') check: (R')</td>
</tr>
<tr>
<td>After (t_{\text{switch}})</td>
<td>Impossible</td>
</tr>
<tr>
<td>Case (e) encrypt (G_1;R'), encrypt (G_2;R') check: (R')</td>
<td></td>
</tr>
</tbody>
</table>

[0033] Switching the randomizers is preferably done periodically, provided that the validity period of a randomizer is greater than \(\Delta T\) 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 \(R_G\) 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 \(R_G\) on a smartcard and copy it from the smartcard into both RSSes) 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 IGC 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>
<thead>
<tr>
<th>Component</th>
<th>Key / Data Item</th>
<th>(Cryptographic) Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roadside System</td>
<td>Secret signature key (SK_G)</td>
<td>Confidential (inside a tamper-proof device)</td>
</tr>
<tr>
<td>Roadside system's</td>
<td>public key(s) (PK_G)</td>
<td>Authentic (certified)</td>
</tr>
<tr>
<td>Operator</td>
<td>Secret signature key (SK_{\text{tap},op})</td>
<td>Confidential (inside a tamper-proof device, access is PIN-protected</td>
</tr>
<tr>
<td>Secret decryption</td>
<td>key (SK_{\text{op}})</td>
<td>Confidential (same as (SK_{\text{tap},op}))</td>
</tr>
<tr>
<td>Key-Generation</td>
<td>Operator's public encryption key (PK_{\text{op}})</td>
<td>Authentic (certified)</td>
</tr>
<tr>
<td>Center</td>
<td>Operator's public signature verification</td>
<td>key (PK_{\text{tap},op})</td>
</tr>
</tbody>
</table>

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 least in order to thwart attacks based on parameter manipulation.

Table 4: System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Semantics and Description</th>
<th>Owner</th>
<th>Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>PK&lt;sub&gt;g&lt;/sub&gt;</td>
<td>Public signature key of each roadside system. Needed to authenticate data submitted to the operator for verification.</td>
<td>Roadside system (specific for each gantry)</td>
<td>Public</td>
</tr>
<tr>
<td>SK&lt;sub&gt;g&lt;/sub&gt;</td>
<td>Secret signature creation key of a roadside system. Needed to digitally sign any payload handed over to the operator.</td>
<td>Roadside system (specific for each gantry)</td>
<td>Secret</td>
</tr>
<tr>
<td>PK&lt;sub&gt;op&lt;/sub&gt;</td>
<td>Public encryption key of the operator. Used by the KGC to secretly deliver a secret key upon a request.</td>
<td>Operator</td>
<td>Public</td>
</tr>
<tr>
<td>SK&lt;sub&gt;op&lt;/sub&gt;</td>
<td>Secret decryption key of the operator. Used to decipher the encrypted secret key for IBE.</td>
<td>Operator</td>
<td>Secret</td>
</tr>
<tr>
<td>PK&lt;sub&gt;SP, op&lt;/sub&gt;</td>
<td>Public signature key of the operator. Used to verify the authenticity of queries to the KGC.</td>
<td>KGC</td>
<td>Public</td>
</tr>
<tr>
<td>SK&lt;sub&gt;SP, op&lt;/sub&gt;</td>
<td>Secret signature key of the operator to authenticate queries to the KGC.</td>
<td>Operator</td>
<td>Secret</td>
</tr>
<tr>
<td>PG</td>
<td>A prime number to create encryption keys within a roadside system.</td>
<td>Roadside system (same for all cooperating gantries)</td>
<td>Public</td>
</tr>
<tr>
<td>g</td>
<td>Generating element of the finite group Z*&lt;sub&gt;PG&lt;/sub&gt; with modulo multiplication.</td>
<td>Every (cooperating) component in the system</td>
<td>Public</td>
</tr>
<tr>
<td>IBE System parameters</td>
<td>See D. Boneh and M. Franklin, t.c.</td>
<td>Roadside system (same for all cooperating gantries) and the key-generation center</td>
<td>Public, except for the KGC master-key.</td>
</tr>
</tbody>
</table>
to a brute-force search over a set of $2^n$ 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 rho algorithm, 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

<table>
<thead>
<tr>
<th>Bit-strength</th>
<th>Size of group (prime)</th>
<th>Size of Integer or Finite Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>160</td>
<td>1024</td>
</tr>
<tr>
<td>112</td>
<td>224</td>
<td>2048</td>
</tr>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
</tr>
<tr>
<td>192</td>
<td>384</td>
<td>7168</td>
</tr>
<tr>
<td>256</td>
<td>512</td>
<td>15360</td>
</tr>
</tbody>
</table>

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 ($PK_{I_B}$), 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 ($PK_{I_B}$), 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 ($PK_{I_B}$), 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 ($PK_{I_B}$), 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 ($PK_{I_B}, PK_{I_B}$), 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 ($SK_{I_B}, SK_{I_B}$) for at least one of said IBE public keys ($PK_{I_B}$, $PK_{I_B}$) from the key generation center (KGC), decrypting at least one of said encrypted session keys ($EK$) with said private key ($SK_{I_B}, SK_{I_B}$), 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 ($R$) which is incorporated into the first identity to generate the first IBE public key ($PK_{I_B}$) and into the second identity to generate the second IBE public key ($PK_{I_B}$).

6. The method of claim 5, wherein the first IBE public key ($PK_{I_B}$) is generated in the form
$PK_{1,1} := g^{((LPN||pub||t)\oplus R_{0})b}\mod p_{G}$

with

$PK_{1,1}$ being the first IBE public key,
$LPN, \ t$ being the identifier and timestamp of the first evidence data,
$R_{0}$ 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

$PK_{2,1} := g^{((LPN||ped||t)\oplus R_{0})b}\mod p_{G}$

with

$PK_{2,1}$ being the second IBE public key,
$LPN, \ t$ being the identifier and timestamp of the second evidence data,
$R_{0}$ 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

$PK_{1,1} \cdot PK_{1,1}^{-1} \mod p_{G}$.

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 $(R_0)$ to a subsequent pseudorandom value $(R_0)$ in a series of pseudorandom values $(R_0)$.

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 $(SK_{D})$ of the first roadside system $(G_1)$, and the second evidence data $(D)$ is cryptographically signed with a signature key $(SK_{D})$ 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 $(PK_{1,1}, PK_{2,1})$, 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 $(\Delta T)$.

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 \((PK_1)\) is sent to the second roadside system \((G_2)\) or the second IBE public key \((PK_2)\) is sent to the first roadside system \((G_1)\) for calculating the ratio \((V)\).
FREMgangsmåde til detektering af et køretøj
Hastighedsovertrædelse
Patentkrav

1. Fremgangsmåde til detektering af en hastighedsovertrædelse, der begås af
et køretøj, som kører fra et første vejsidesystem (G₁) til et andet vejsidesystem (G₂),
hvilken fremgangsmåde består af:

Opsætning af private og offentlige parametre (g, P₀₀), inklusive en fælles modulo-basis
(P₀), for en identitets-baseret kryptering (IBE), en ordning i et nøglegenereringscenter
(KGC) samt det første og det andet vejsidesystem (G₁, G₂);

Registrering af mindst en identifikator (LPN) for køretøjet og et første tidsstempel (t) ved
det første vejsidesystem (G₁) som første sæt bevisdata (D) ved hjælp af mindst den
første identifikator (LPN) og det første tidsstempel (t) som en første identitet for at
generere en første IBE-offentlig nøgle (PK₁₁), kryptering af det første sæt bevisdata (D)
med en første tilfældig sessionsnøgle (K), kryptering af den første tilfældige
sessionsnøgle (K) med den første IBE-offentlige nøgle (PK₁₁) samt sletning af det første
sæt bevisdata (D) og den første tilfældige sessionsnøgle (K) ved det første
vejsidesystem (G₁);

Registrering af mindst en identifikator (LPN) for køretøjet og et andet tidsstempel (t) ved
det andet vejsidesystem (G₂) som andet sæt bevisdata (D) ved hjælp af mindst den
anden identifikator (LPN) og det andet tidsstempel (t) som en anden identitet for at
generere en anden IBE-offentlig nøgle (PK₂₁), kryptering af det andet sæt bevisdata (D)
med en anden tilfældig sessionsnøgle (K), kryptering af den anden tilfældige
sessionsnøgle (K) med den anden IBE-offentlige nøgle (PK₂₁) samt sletning af det andet
sæt bevisdata (D) og den anden tilfældige sessionsnøgle (K) ved det andet
vejsidesystem (G₂);

beregning af et forhold (V) mellem den første og den anden offentlige nøgle (PK₁₁, PK₂₁),
modulo den fælles modulo-base (P₀) og opslag af forholdet (V) i en tabel over forhold
(V), som er forudberegnet for et sæt tidsforskelle mellem nævnte første og andet
tidsstempel (t), hvilket sæt repræsenterer hastighedsovertrædelser og, når opslaget er
succesfuldt;
indhentning af mindst én IBE-privat nøgle (SK₁, SK₂) for mindst én af nævnte IBE-offentlige nøgler (PK₁₂, PK₂₁) fra nøglegenereringscentret (KGC), kryptering af mindst én af nævnte krypeterede sessionsnøgler (EK) med nævnte private nøgler (SK₁, SK₂) samt kryptering af mindst én af nævnte krypeterede sæt bevisdata (ED) med nævnte krypeterede nøgler (K).

2. Fremgangsmåde ifølge krav 1, hvor IBE-ordningen er en Boneh-Franklin-krypeteringsordning.

3. Fremgangsmåde ifølge krav 1 eller 2, hvor bevisdataene (D) krypeteres med sessionsnøglen (K) ifølge en symmetrisk krypeteringsordning.

4. Fremgangsmåde ifølge krav 3, hvor den symmetriske krypeteringsordning er den avancerede krypeteringsstandard (AES).

5. Fremgangsmåde ifølge et af kravene 1 til 4, hvor det første og det andet vejsidesystem (G₁, G₂) deler mindst én tilfældig eller pseudo-tilfældig værdi (R₁), som inkorporeres i den første identitet for at generere den første IBE-offentlige nøgle (PK₁₁) og i den anden identitet for at generere den anden IBE-offentlige nøgle (PK₂₂).

6. Fremgangsmåde ifølge krav 5, hvor den første IBE-offentlige nøgle (PK₁₁) genereres via formlen

\[ PK_{11} = g^{(\text{LPN} \| \text{pad} \oplus R₁)} \mod p_G \]

Hvor

PK₁₁ er den første IBE-offentlige nøgle,

LPN,₁ er identifikatoren og tidsstemplet for det første sæt bevisdata,

R₁ er den tilfældige eller pseudo-tilfældige værdi,

g, PG er de offentlige parametre for IBE-ordningen,

mens den anden IBE offentlige nøgle genereres via formlen

\[ PK_{22} = g^{(\text{LPN} \| \text{pad} \oplus R₂)} \mod p_G \]
Hvor
PK₂ₜ er den anden IBE-offentlige nøgle,
LPN,₁ er identifikatoren og tidsstemplet for det andet sæt bevisdata,
R₁ er den tilfældige eller pseudo-tilfældige værdi,
g, PG er de offentlige parametre for IBE-ordningen,

7. Fremgangsmåde ifølge krav 6, hvor forholdet (V) beregnes via formlen
   \[ PK₂ₜ \cdot PK₁ₜ⁻¹ \pmod{p₀} \] .

8. Fremgangsmåde ifølge et af kravene 5 til 7, hvor det første og det andet vejsidesystem (G₁, G₂) kommunikerer for synkroniseret at skifte fra én pseudo-tilfældig værdi (R₁) til en efterfølgende pseudo-tilfældig værdi (R₁) i en serie af pseudo-tilfældige værdier (R₁).

9. Fremgangsmåde ifølge et af kravene 1 til 8, hvor det første sæt bevisdata (D) omfatter et billede (PIC) af køretøjet, som tages med et kamera ved det første vejsidesystem (G₁), og det andet sæt bevisdata (D) omfatter et billede (PIC) af køretøjet, som tages med et kamera ved det andet vejsidesystem (G₂).

10. Fremgangsmåde ifølge et af kravene 1 til 9, hvor det første sæt bevisdata (D) krypteres grafisk signeret med en signaturnøgle (SKG) i det første vejsidesystem (G₁), og hvor det andet sæt bevisdata (D) signeres kryptografisk med en signaturnøgle (SK₀) i det andet vejsidesystem (G₂).

11. Fremgangsmåde ifølge et af kravene 1 til 10, hvor sessionsnøglen (K) har mindst 128 bits.

12. Fremgangsmåde ifølge et af kravene 1 til 11, hvor den første og den anden IBE-offentlige nøgle (PK₁ₜ, PK₂ₜ), den krypterede og anden sessionsnøgle (EK) og det krypterede første og andet sæt bevisdata (ED) slettes efter en forudbestemt periode (ΔT).
13. Fremgangsmåde ifølge et af kravene 1 til 12, hvor det første sæt bevisdata (D) omfatter en klasse (VC) af det køretøj, som registreres ved det første vejsidesystem (G₁).

14. Fremgangsmåde ifølge krav 13, hvor der forudberegnes forskellige tabeller over forhold (V) for forskellige klasser (VC) af køretøjer, og hvor den tabel, der anvendes til opslag, vælges i henhold til køretøjets klasse.

15. Fremgangsmåde ifølge et af kravene 1 til 14, hvor det første og det andet sæt bevisdata (D) omfatter en vejrligs- eller vejtilstand (AD), som registreres ved det første eller andet vejsidesystem (G₁, G₂), og hvor der forudberegnes forskellige tabeller over forhold (V) for forskellige tilstande, og hvor den tabel, der anvendes til opslag, vælges i henhold til den registrerede tilstand.

16. Fremgangsmåde ifølge krav 1 til 15, hvor den første IBE-offentlige nøgle (PK₁₁) sendes til det andet vejsidesystem (G₂) eller den anden IBE-offentlige nøgle (PK₂₁) sendes til det første vejsidesystem (G₁) for at beregne forholdet (V).
Fig. 3
### Fig. 4

<table>
<thead>
<tr>
<th>RSS</th>
<th>enc</th>
<th>( t_{\text{switch}} - \Delta T )</th>
<th>( \Delta T )</th>
<th>( t_{\text{switch}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>( R )</td>
<td>( R ) and ( R' )</td>
<td>( R' )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( R )</td>
<td>( R ) or ( R' )</td>
<td>( R' )</td>
</tr>
</tbody>
</table>

**Gantry \( G_1 \) check**

- (a)
- (b)
- (c)
- (d)
- (e)

**Gantry \( G_2 \)**

<table>
<thead>
<tr>
<th>RSS</th>
<th>enc</th>
<th>( R )</th>
<th>( R' )</th>
</tr>
</thead>
</table>

| RSS | enc | \( R' \) | \( R' \) |

**Gantry \( G_2 \)**