results in No, the control portion 220 terminates the process in FIG. 4. When the determination at S8 also results in Yes, the control portion 220 proceeds to S10.

[0071]

At S10, the control portion 220 generates a hash value from the hash function using the H matrix as data generated by the authentication center 120 and the parity data, as input keys. The hash value corresponds to authenticated data of the present disclosure.

[0072]

At S12, the control portion 220 transmits the position information indicating the present position computed at S2, the hash value generated at S10, and PRNID and TOW extracted at S44 to the communication portion 310 of the roadside apparatus 300 from the transmission portion 212.

[0073]

(Processes in the roadside apparatus 300)

The control portion 320 of the roadside apparatus 300 cyclically transmits a request signal that requests to transmit position information around the roadside apparatus 300. When the vehicle onboard apparatus 200 receives the request signal, the vehicle onboard apparatus 200 transmits the position information, the hash value, or the like as described above.

[0074]

The control portion 320 of the roadside apparatus 300 performs a process illustrated in FIG. 7 when the communication portion 310 of the roadside apparatus 300 receives the position information, the hash value, or the like from the vehicle onboard apparatus 200.

[0075]

At S70, the control portion 320 acquires the position information, the hash value, PRNID, and TOW received by the communication portion 310 from the communication portion 310. The process at S70 corresponds to a terminal data acquisition portion of the present disclosure.

[0076]

At S72, the control portion 320 transmits PRNID and TOW acquired at S70 along with a public key to the authentication center 120 from the

receives position information and an authenticated data from a positioning terminal that wirelessly transmits the position information and the authenticated data outside, the position information indicating the present position computed using the navigation message, the authenticated data indicating the navigation message that has been received is authenticated, the position information acquisition apparatus comprising:

a terminal data acquisition portion that acquires the position information and the authenticated data transmitted by the positioning terminal from a communication portion;

a key acquisition portion that allows the communication portion to acquire a key-related data from an authentication center apparatus, wherein the key-related data corresponds to one of a cryptography key and a key generation data, the cryptography key being used by the authentication center apparatus to generate a center-generated authentication data that is used by the positioning terminal for authentication, the key generation data being capable of generating the cryptography key;

a comparative data generation portion that generates an authenticated comparative data to be compared with the authenticated data based on the key-related data acquired by the key acquisition portion; and

a terminal determination portion that compares the authenticated data acquired by the terminal data acquisition portion with the authenticated comparative data generated by the comparative data generation portion and, when the authenticated data acquired by the terminal data acquisition portion is matched with the authenticated comparative data generated by the comparative data generation portion, determines that the positioning terminal is a regular positioning terminal.

7. The position information authentication system according to claim 2, wherein:

the authenticated data generation portion generates the authenticated data by the hash function using the center-generated authentication data along with the key-related data received by the key reception portion.