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

(11) EP 1 017 025 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.07.2000 Bulletin 2000/27

(51) Int Cl.[7]: **G07C 13/00**

(21) Application number: **99250450.6**

(22) Date of filing: **28.12.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **28.12.1998 JP 37176898**

(71) Applicant: **NEC CORPORATION**
Tokyo (JP)

(72) Inventor: **Sako, Kazue**
Minato-ku, Tokyo (JP)

(74) Representative: **Patentanwälte Wenzel & Kalkoff**
Grubesallee 26
22143 Hamburg (DE)

(54) Receipt-free electronic voting method and system

(57) A method of effectively providing, with minimum physical limitation, a secure receipt-free protocol which does not supply a receipt which proves contents of voting action to a voter. A vote generating center and a converting center generate voting data and send them to each vote selecting device. Then, each vote selecting device selects its own vote based on the voting data. When a counting center counts the vote, the voting data are converted to a new configuration of data or existing voting data and the correctness of the configuration or the conversion is proved. Further, correspondence of the configuration or the conversion is sent only to the vote selecting device via an anti-eavesdropping channel.

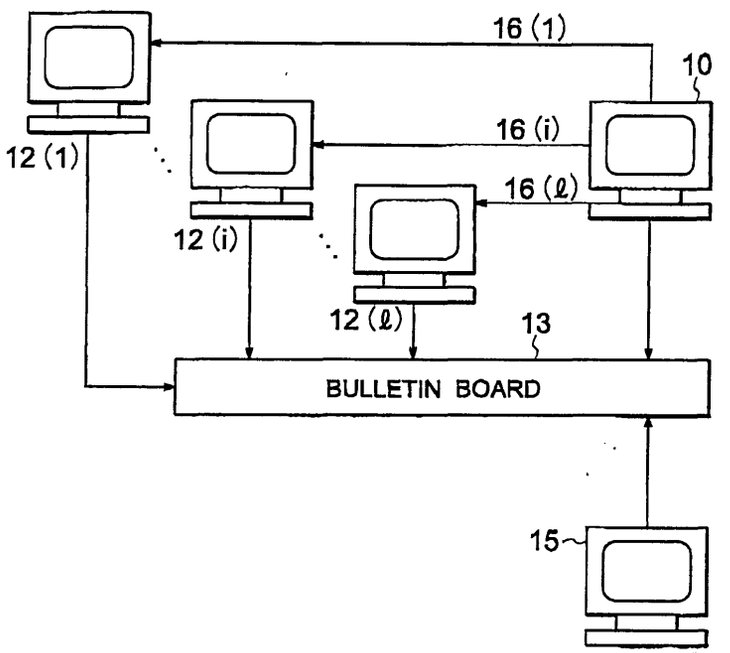

FIG. 1

EP 1 017 025 A2

Description

BACKGROUND OF THE INVENTION:

Field of the Invention

[0001] The invention relates to an advantageous receipt-free electronic voting method and system, in particular, to an algorithm which is based on number theory and which is used for a secure receipt-free electronic voting system.

Description of the Related Art

[0002] In most of electronic voting protocols, a receipt which represents a fact that a voter casts a ballot for a candidate is provided, unlike previous non-electronic voting protocols. Due to the existence of the receipt, a voter may sell his/her ballot, or a third party may force a voter to cast a ballot for a specific candidate.

[0003] Therefore, to overcome the shortcomings of electronic voting protocols, a first receipt-free electronic voting protocol has been proposed which is disclosed in an article by J. C. Benaloh et, al., entitled "Receipt-free Secret-ballot Election," in STOC94, 1994, pp. 544 to 553.

[0004] In the protocol, a trusted center generates for each voter a pair of ballots consisting of a "yes" vote and a "no" vote in random order. Using a trusted beacon and a physical voting booth, the center proves to the public that the ballot indeed includes a well-formed (yes/no) or (no/yes) pair and at the same time proves to the verifier which pair it is. The physical apparatus ensures that by the time the verifier is able to communicate with an outsider, the verifier can forge a proof that the ballot is (yes/no) and also forge a proof that it is (no/yes). Thus, such a proof cease to provide either proof as a receipt.

[0005] Independently, Niemi and Renvall tried to solve this problem in an article by Niemi and Renvall, entitled "How to prevent buying of votes in computer elections," in ASIACRYPT '94, 1994, pp. 141 to 148. They also use a physical voting booth where a voter performs multiparty computation with all the centers.

[0006] In the first and second protocols, however, there is required a one-way anti-eavesdropping secure channel.

[0007] Alternatively, a third receipt-free electronic voting protocol disclosed in Japanese Laying-Open Publication No. H08-315053 (namely, 315053/1996). The third protocol includes the following three steps. The first step is to publish, at a vote generating center, a set of voting slips which include all votes corresponding to possible candidates, to each voter. The second step is to transfer the voting slips to the voter from the vote generating center via a shuffling center. The third step is to perform anonymous voting by the voter. Each voter can see which voting slip corresponds to a specific voting action by storing an original arrangement of the set of the voting slips and a result of shuffling in the second step. Each voter submits one of the voting slips received to a counting center via a secure anonymous channel. Then, the counting center counts up the number of the submitted voting slips.

[0008] In the third protocol is required a one-way secure anti-eavesdropping channel which prevents from eavesdropping along with the route from the vote generating center to a vote selecting device. However, there is required an anonymous channel to send a voting message from the vote selecting device to the counting center. Further, the amount of computational complexity of the anonymous channel is proportional to the number of voters. Therefore, to realize communication through the anonymous channel, a great amount of computational complexity is required.

[0009] Further, a fourth receipt-free electronic voting protocol has been proposed such as disclosed in an article by Okamoto, entitled "Receipt-free electronic voting schemes for large scale elections" in Security Protocols '97, pp. 25 to 35 or disclosed in Japanese Laying-Open Publication No. H10-74182(namely, 74182/1998). According to the fourth protocol, a secure receipt-free voting method is achieved using a secure anonymous channel between a voter and a counting center.

[0010] In the fourth protocol, however, a physically secure anonymous channel is required, but its existence is unknown.

SUMMARY OF THE INVENTION:

[0011] Therefore, it is an object of the invention to provide a secure receipt-free electronic voting method using a one-way anti-eavesdropping channel rather than an anonymous channel having a great amount of computational complexity.

[0012] According to the secure receipt-free electronic voting method of the present invention, by using physically secure and anti-eavesdropping channel, evidence of each voter's voting action does not remain. Herein, terms "a secure and anti-eavesdropping channel" mean that the channel can transfer messages from a center without a third party's access or detection of the messages.

[0013] Such an anti-eavesdropping channel is disclosed in an article by C. Bennett et. al., entitled "Quantum Cryptography" in Scientific American, Oct. 1992, vol. 267 no. 4, pp. 50 to 57. Major effect of introducing the anti-eavesdropping channel is that any people including voters and third parties cannot prove the fact that they vote for a specific candidate or they send a specific content of messages. Once the messages are sent or received, the contents of the messages are changed and it is not possible to output their proofs. However, if the messages are monitored or detected on the way or on their reception, one who monitors or detects the messages can see the contents of the mes-

sages before a time point when the messages can be changed. Furthermore, according to the present invention, even if a non secure channel is used, when the messages are transferred via the channel without monitoring or detecting, it is impossible to see the contents of the messages, for example, contents of voting, once the messages are received by a destination node. In other words, anti-eavesdropping channel serves to transfer messages without monitoring or detecting on the way.

[0014] In the following description, terms "designated-verifier proofs" are used. The designated-verifier proof is a protocol which proves by using a public key of a verifier etc. According to the protocol, a verifier understand the correctness of proofs, but a person other than the verifier can not understand the correctness of the proofs even if the verifier transfers the proofs received by himself/herself to the person.

[0015] More detail description and concrete construction are made in an article by Jakobsson, Sako, and Impagliazzo, entitled "Designated-verifier proofs and their applications" in Advances in Cryptology, Eurocrypt '96, 1996, pp. 143 to 154.

[0016] According to a first embodiment of the invention, a receipt-free electronic voting method comprises four steps. The first step is publishing, at a vote generating center, voting data to each voter. The voting data is configured so that all of possibles choices for voting may be selected. Herein, it is assumed that there are L choices. The vote generating center produces the voting data for each voter i and proves that the voting data are produced correctly. Further, the vote generating center transmits contents of the voting data only to the voter via a secure anti-eavesdropping channel and proves that the correspondence of the voting data to the voter is correct by using the designated-verifier proofs protocol.

[0017] The second step is transferring, at the vote generating center, the voting data to the voter via a converting center. Each converting center converts the voting data corresponding to a voter i via a conversion network, as a result, outputs a converted voting data.

[0018] The converting center proves correctness of the operation, that is, proves that the converted voting data are correctly produced by converting the received voting data using proper conversion parameters. Further, how the received data are converted and a part of the conversion parameters are transferred only to the voter via the secure anti-eavesdropping channel, and proves that the conversion is correctly performed by using the designated-verifier proofs protocol.

[0019] The second step is optional; if the step is omitted, the vote generating center directly transfers the voting data to the voter via a bulletin board.

[0020] The third step is voting by a voter. By storing contents of the original voting data and how the voting data are converted in the second step, each voter can find that how the voter should select data corresponding to the object which the voter wants to vote for among the voting data. Each voter selects the data corresponding to object which the voter wants to vote for as voted data, and submits the voted data to a counting center via the bulletin board.

[0021] The fourth step is counting, at the counting center, the voted data. The counting center accumulates the voted data of each voter keeping encrypted. To count the votes, the accumulated and encrypted data are decrypted. Such a vote counting method is, for example, described in an article entitled "A secure and optimally efficient multi-authority election scheme" in Advances in Cryptology, Eurocrypt'97, 1997, pp. 103 to 118. As described in the article, it is preferable to properly control decrypting authority at the counting center so that the counting center may not decrypt each of the encrypted and voted data and as a result, leak a secret of the encrypted and voted data. A number of methods has been proposed for such an object. One of the methods is explained in an article entitled "A Threshold Cryptosystem without a Trusted Party" in Advances in Cryptology, Eurocrypt '91, 1991, pp. 522 to 526.

[0022] Thereby, a voter cannot publish a receipt which proves the contents of voting because the voter cannot prove to a third party the contents of the voting data which are produced by the vote generating center and the converting center.

[0023] Furthermore, it is ensured that a vote which is selected by a voter is correct because the vote generating center and each of the converting centers prove that the voting data are correctly produced and converted.

[0024] Still further, if the second step is performed, the contents of voting are concealed also to the vote generating center because each of the converting centers converts the voting data which are produced by the vote generating center.

[0025] Also, a set of encrypted votes representing all of possible choices for voting may be used as the voting data including all possible choices for voting. Correspondence between the encrypted votes and the choices for voting may be used as contents of voting data. Herein, the voting data may be converted by switching the sequence in the set of the encrypted votes. Thus, contents of converted voting data are represented by the switched order.

[0026] Alternatively, an encrypted vote representing a choice for voting may also be used as voting data. In this case, by changing a converting parameter, another choice for voting may be selected.

[0027] Even if the voting data are not directly related to the encrypted votes, the voting data may represent all choices for voting by converting the voting data. That is, even if the same vote is selected, different representation of the vote can be achieved by employing different generating methods and different selecting methods.

[0028] According to a first aspect of the invention, a receipt-free electronic voting method is provided. The

method comprises the steps of (a) generating voting data and posting them to a bulletin board, (b) sending a secret message to a vote selecting device without being monitored, (c) selecting, at the selecting device, a vote using the voting data on the bulletin board, and (d) counting, at a counting center, the votes.

[0029] According to a second aspect of the invention, a receipt-free electronic voting system is provided. The system comprises one or more vote generating centers, a plurality of vote selecting devices, a bulletin board, and a vote counting center. Furthermore, the vote generating center generates voting data, posts them to the bulletin board, and sends a secret message to each vote selecting device without being monitored, each of the vote selecting devices selects a vote using the voting data via the bulletin board, and the vote counting device counts the votes.

[0030] According to a third aspect of the invention, a recording medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform a receipt-free electronic voting method is provided. Herein, the method comprises the steps of (a) generating voting data and posting them to a bulletin board, (b) sending a secret message to a vote selecting device without being monitored, (c) selecting, at the selecting device, a vote using the voting data on the bulletin board, and (d) counting, at a counting center, the votes.

BRIEF DESCRIPTION OF THE DRAWINGS:

[0031]

Fig. 1 shows a block diagram of a first embodiment of the invention;

Fig. 2 shows flows of a message according to the first embodiment of the invention;

Fig. 3 shows a block diagram of a second embodiment of the invention including converting centers;

Fig. 4 shows flows of a message according to the second embodiment of the invention including converting centers; and

Fig. 5 shows a block diagram of the converting center.

DESCRIPTION OF THE PREFERRED EMBODIMENT:

[0032] At first, description is made about a secure receipt-free electronic voting method according to a first embodiment of the invention with reference to Figs. 1 and 2. In fig. 1, a plurality of vote selecting devices 12 (i), a vote generating center 10, and a vote counting center 15 are connected to a bulletin board 13 via, for example, the internet. The vote generating center 10 is also connected to each of the vote selecting devices 12 (i) via an anti-eavesdropping channel 16(i).

[0033] In fig. 2, the vote generating center 10 includes proving process 20, data configuring process 26, and contents transferring process 28. The contents transferring process 28 employs a contents proofs algorithm 22. The vote selecting center 12(i) includes a verifying process 24, a selecting process 25, and an invalidating process 27.

[0034] Herein, for the sake of simplification, it is assumed that voting is allowed to be chosen on either a vote "1" or a vote "0". Voting data is also assumed to be composed of a random sequence of a pair of the vote "1" and the vote "0" subjected to rearrangement and to be given to each of the vote selecting device 12(i). The vote generating center 10 publicly proves that the voting data are correctly generated. This proving is performed by the proving process 20. Further, contents of the voting data to the vote selecting device 12(i), (that is, how the votes are arranged) are transferred in secret to the vote selecting 12(i) via an anti-eavesdropping channel 16(i). Simultaneously, the vote generating center 10 proves that the contents are correct via the anti-eavesdropping channel 16(i).

[0035] The transferring and proving are performed by the contents transferring process 28 in a manner to be described later.

[0036] The vote selecting device 12(i) is also given secret messages sent from the vote generating center 10 via a physically anti-eavesdropping channel 16(i) and selects its own vote with reference to the secret messages by the use of the voting data. The vote which is selected by the vote selecting devices 12(1), 12(2),..., 12(1), is encrypted into an encrypted vote and is transferred to the vote counting center 15 through the bulletin board 13. All of the encrypted votes are accumulated at the vote counting center 15. The vote counting center 15 decrypts the accumulated and encrypted votes to detect results of voting. Each of the vote generating center 10, the vote selecting devices 12(l), and the vote counting center 15 may be preferably implemented by a personal computer, but may be a workstation or the like.

[0037] Next, more detailed description is made about information which is safely transferred via the data configuring process 26, the proving process 20, the contents transferring process 28, and the anti-eavesdropping channels 16.

[0038] The vote generating center 10 generates voting data, that is, a set of encrypted votes including the vote "0" and the vote "1" by executing the data configuring process 26. The center 10 executes the data configuring process 26 for each vote selecting device 12(i) by individually using a selected random number.

[0039] Encryption of the vote "0" and the vote "1" should be adapted to be supplied to the bulletin board 13. Preferably, the vote "0" and the vote "1" may be encrypted by using a method disclosed in the above mentioned article "A Secure and Optimally Efficient Multi-Authority Election Scheme".

[0040] More specifically, it is assumed that each of constants p, g, h, G is at first determined as a common constant selected for all vote selecting devices in the

manner mentioned in the above referenced article.

[0041] Next, a re-encryption scheme is defined. Supplied with an input v = (x, y), the scheme generates v'= (x g^ α mod p, y h^ α mod p) by using the selected random number α. Decrypting the equation v = (x, y) can be accomplished by counting out calculation (y/x^z mod p), where z satisfies (h = g^z mod p). This shows that a result of decrypting the re-encrypted v' is equal to v. On the other hand, because the random number α is used to convert v to v', a relationship between v and v' can be concealed for people who do not know about the value of the α.

[0042] Thus, the definition is made about the fact that the aspect of encrypting the vote "1" indicates all results obtained by re-encrypting v1 = (1, G) while the aspect of encrypting the vote "0" indicates all results obtained by re-encrypting v0 = (1, 1/G).

[0043] Before detailed description of the data configuring process 26, brief description is made of a method of counting or accumulating. When thus produced and encrypted votes are counted up, calculation is counted out to obtain each of products among the first elements of the encrypted aspect and each product among the second elements. Thus obtained and encrypted totals (X, Y) are calculated with a secret key of the counting center. As a result of the calculating Y / X^z mod p, G^T mod p is obtained. Herein, T is the difference between the total number of the votes "1" and the total number of the votes "0", the vote "1" is a majority if T is a positive number, the vote "0" is a majority if T is a negative number. As described above, counting of the votes may be performed.

[0044] Hereinafter, major parts of the invention, that is, a method of generating of voting data and an electronic voting method are described in more detail. The vote generating center 10 re-encrypts the v1 and v0 using the randomly selected random numbers ri1 and ri2, respectively, and generates vi1 and vi0 in the data configuring process 26.

[0045] The vote generating center 10 transfers the set of voting data (viA, viB) to the bulletin board. Herein, each of viA and viB may take vi0 or vi1, and the set (viA, viB) takes the order (vi0, vi1) with probability of 1/2. Similarly, the set (viA, viB) takes the order (vi1, vi0) with probability of 1/2. In the proving process 20, the vote generating center 10 proves that the result of re-encrypting the vote "1" is either of (viA, viB) and the result of re-encrypting the vote "0" is either of (viA, viB). This operation proves that the voting data (viA, viB) supplied from the vote generating center 10 consists of a correct vote "1" and a correct vote "0". Specifically, description will be made in conjunction with the OR proofs algorithm which proves the result of re-encrypting v is equal to either v1 or v2.

[0046] Next, description is made about the contents transferring process 28. The process 28 correctly transfers the contents of voting data which may includes the order (vi1, vi0) or (vi0, vi1) to one of the vote selecting devices 12(i) via the anti-eavesdropping channel 16. To prove that the voting data are correctly transferred, it is required to prove result of re-encrypting a vote "1" is viA and result of re-encrypting a vote "0" is viB when A = 1 and B = 0, or to prove result of re-encrypting a vote "1" is viB and result of re-encrypting a vote "0" is viA when A = 0 and B = 1. Further, the proofs are performed by designated-verifier proofs using a public key of the vote selection device 12(i).

[0047] Also, in this case, because the prove process 20 separately proves that (viA, viB) is a correct set of encrypted votes if it is only shown that result of re-encrypting the vote "1" (or the vote "0") is viA, that result of re-encrypting the vote "0" (or the vote "1") is viB automatically holds.

[0048] A re-encryption proof algorithm is described below in more detail which proves that the result of re-encrypting v is v' using designated-verifier proofs.

[0049] As described above, the vote generating center transfers the contents of voting data and designated-verifier proofs representing its correctness to the vote selecting device 12(i) via the anti-eavesdropping channel 16.

[0050] The vote selecting device 12(i) verifies the correctness of the contents proofs algorithm using the verifying process 42. If the correctness is verified, the vote selecting device 12 (i) executes the selection process 25 and selects one among the voting data consisting of a set of encrypted votes in the bulletin board. The vote selecting device can select correctly because the device is informed of the arrangement of the encrypted data included in the voting data by the contents transferring process.

[0051] Votes selected by the vote selecting device 12 (i) are supplied to the vote counting center 15 as well as the other votes selected by the other vote selecting device.

[0052] Applying the above method, even if malicious people force the vote selecting device 12(i) to disclose the votes, concrete evidence may not be obtained that whether the selected vote includes a vote "1" or a vote "0", as long as a vote generating center 10 allows votes to disclose or an anti-eavesdropping channel 16(i) is eavesdropped.

[0053] Next, description is made about an OR proofs algorithm and a designated-verifier re-encryption proofs algorithm. Both of the algorithms include proving a device and a verifying device. In this case, the proving device is a vote generating center. The verifying device is a vote selecting device when the designated-verifier re-encryption proofs algorithm is used, or is a public including the vote selecting device when the OR proofs algorithm is used. In these algorithms, a proofs protocol holds by using a proper hash function H even if the proving device and the verifying device do not communicate with each other.

[0054] OR proofs algorithm

(Proving that the result of re-encrypting v (= (x, y))

v1 (= (x1, y1)) or V^2 (= (x2, y2)))

[0055] Herein, the proving device knows j and α (xj = x g α mod p, yj = y h α mod p).

1. The proving device randomly selects d1, d2, r1, r2, and calculates the following equations.

a1 =(x1/x)^d1 * g^r1 mod p

a2 =(x2/x)^d2 * g^r2 mod p

b1 =(y1/y)^d1 * h^r1 mod p

b2 =(y2/y)^d2 * h^r2 mod p

2. The proving device calculates the following equation.

c.= H(x, y, x1, y1, x2, y2, a1, a2, b1, b2).

3. If the result of re-encrypting v is equal to vj, dj is replaced with c-dj' (j' is the number other than j) and rj is replaced with αd'+rj-αdj (d' is dj before it is replaced).
4. Thus replaced d1, d2, r1, r2 are defined as proofs.
5. The verifying device recalculates the following equations based on the received d1, d2, r1, r2.

a1 =(x1/x)^d1 * g^r1 mod p

a2 =(x2/x)^d2 * g^r2 mod p

b1 =(y1/y)^d1 * h^r1 mod p

b2 =(y2/y)^d2 * h^r2 mod p

[0056] Next, the verifying device verifies whether the following equation holds or not.

d1 + d2 = H(x, y, x1, y1, x2, y2, a1, a2, b1, b2).

[0057] The OR proofs algorithm may be embodied by the other method as long as it is proved that the result of re-encrypting v = (x, y) is v1 = (x1, y1) or v2 = (x2, y2). For example, it may be not like the above proofs algorithm using a hash function but like an interactive proofs algorithm having a verifying device which selects c at random. Moreover, the proving process 20 is not a method which employs the above OR proofs algorithm twice but any algorithm which may prove that given voting data can represent all of choices for voting without concretely denoting correspondence relationship to each choice. For example, it may be an algorithm which proves that a result of re-encrypting a vote "1" is either viA or viB with the OR proofs algorithm and then proves that a result of multiplying the viA and viB for each element is equal to a result of re-encrypting (1,1). These variations are easily thought of by those skilled in the art.

[0058] Next, description is made of a designated-verifier re-encrypting proofs algorithm.

[0059] Designated-verifier re-encrypting proofs algorithm (proving that a result of re-encrypting V = (x, y) is v' = (x', y'))

[0060] Herein, it is assumed that a proving device knows α (x' = x g α mod p, y' = y h α mod p). Further, it is assumed that the proving device knows p (h' = g^z' mod p) as a public key of a verifying device.

1. The proving device randomly selects d, w, r, and calculates the following equations.

a = g^d mod p

b = h^d mod p

s =g^w h'^r mod p

2. The proving device calculates the following equation.

c = H(x, y, x', y', a, b, s).

3. The proving device calculates the following equation.

u = d + α(c + w)

4. The values of c, w, r, and u are defined as proofs.
5. The verifying device recalculates the following equations based on the received c, w, r, u.

a = g^u / (x'/x) ^ (c + w) mod p

b = h^u/(y'/y) ^ (c + w) mod p

s = g^w h'^r mod p

[0061] Next, the verifying device verifies whether the

following equation holds or not.

$$c = H(x, y, x', y', a, b, s).$$

[0062] The designated-verifier re-encrypting proofs algorithm may not be the above method. The proofs algorithm may be any method which can prove that a result of encrypting of v = (x, y) is v' = (x', y') and only verifier can assure its validity. Furthermore, the contents transferring process 28 need not use the designated-verifier re-encrypting proofs algorithm. The process 28 can use any algorithm as long as contents of each voting data to be transferred are proved in a manner in which only specific verifiers can recognize the correctness

[0063] Once z' is known, a set of proofs (c, w, r, u) which can pass through a check of the above designated-verifier proofs may be created for pairs of (x, y) and (x', y') which is not always a result of re-encrypting (x, y). Therefore, the designated-verifier proofs algorithm is easily invalidated by informing of z'.

[0064] More detailed description about the designated-verifier proofs algorithm is made in the above mentioned article entitled "Designated-verifier proofs and their applications".

[0065] The vote selecting device 12(i) performs invalidating process 27 to invalidate proofs of the vote generating center after the center sends a secret message. The invalidating process 27 informs the center of a value of z' and makes the center have ability of providing incorrect information later or ability of posting the value of z' to a bulletin board 13.

[0066] To improve security of receipt-free properties, a conversion network 11 including a plurality of converting centers 11(1), 11(2), ...,11(m) may be incorporated, as shown in Figs. 3 and 4. The voting data which are generated by the vote generating center 10 and forwarded to the vote selecting device 12(i) passes through the conversion network 11 before the voting data arrives at the vote selecting device 12(i). In such a configuration, it is impossible to determine how a vote selecting device makes a ballot for malicious people, as long as all of the converting centers and the vote generating center conspire together or anti-eavesdropping channels 17(1), 17 (2),..., 17(m) each of which resides between one of the converting center and one of the vote selecting device 12(i) are all eavesdropped.

[0067] Each of the converting center includes a calculating device, and may be preferably implemented by a personal computer. The center, however, may be a workstation or the like.

[0068] Description is made about operations of the conversion network and the converting centers. The converting center 11(j) sends the result of converting process 30 (shown in Fig. 5) which converts voting data sent from the previous converting center 11 (j-1)(when j=1, it represents the vote generating center 10). The above operation is repeated until the last converting center 11 (m) sends its result. Each of the converting centers informs the vote selecting device of how the voting data are converted via secure anti-eavesdropping channel 17(j). Each of the converting centers proves to the vote selecting device that the conversion is correctly performed and incorrect information is not provided, as similar to the vote generating center. This operation is performed by proving process 31 and correspondence proofs algorithm 33.

[0069] Next, referring to Fig. 5, the converting center 11(i) performs converting process 30 and proving process 31, and sends its output. The proving process 31 proves that conversion is correctly and publicly performed. Correspondence transferring process 32 proves that how the actual conversion is performed and information is not incorrect only to the vote selecting device with the designated-verifier correspondence proofs algorithm 33.

[0070] Next, description is made about the converting process 30. It is assumed that input data to the process are voting data (V1, V2).

[0071] A Converting algorithm re-encrypts the encrypted vote V1 and V2 using generated random numbers c1 and c2, sends the result in random order as VA and VB.

[0072] The proving process 31 is used to prove that the converting center correctly performs the converting algorithm. The proving process 31 includes a proving device and a verifying device. In this case, the proving device is the converting center. The verifying device may be any entity including the vote selecting device. This concretely means that it is satisfied to prove that a result of re-encrypting V1 is either VA or VB, and a result of re-encrypting V2 is either VA or VB by using the above mentioned OR proofs algorithm.

[0073] Proving process may be performed in any algorithm as long as the algorithm can prove that a given set of output cryptogram is produced by replacing a set of input cryptogram without showing concrete replace method. For example, the algorithm may prove that a result of encrypting V1 is either VA or VB by using the OR proofs algorithm, and the result of encrypting (1, 1) is equal to a result of multiplying VA by VB for each element. These variations are easily thought of by those skilled in the art.

[0074] Next, description is made about correspondence transferring process 32. The process correctly communicates with the vote selecting device 12(i) contents of converting (A = 1 and B = 2, or A = 2 and B = 1). The correctness of the contents is ensured by proving that a result of re-encrypting V1 is VA and a result of re-encrypting V2 is VB when A = 1 and B = 2, and that a result of re-encrypting V1 is VB and a result of re-encrypting V2 is VA when A = 2 and B = 1. This may be achieved by executing the above designated-verifier re-encrypting proofs algorithm once.

[0075] Voting data sent from the vote generating center are sequentially processed by the converting center

11(1), 11(2),...,11(m), until the last center sends to each vote selecting device a set of randomly and untraceably arranged and encrypted votes.

[0076] The vote selecting device 12(i) selects a vote using a secret message sent from the vote generating center and the converting center via secure anti-eavesdropping channels 16(i), 17(1), 17(2), ...,17(m). Validating of proofs of the converting center is performed as similar to the validation of proofs of the vote generating center.

[0077] Here, to simplify the description, a voting scheme which selects one from vote "0" and vote "1" is illustrated. However, in a voting scheme which selects one among more than three votes, an aspect of encrypting may be adopted as disclosed in the above article entitled "A Secure and optimally Efficient Multi-Authority Election Scheme", and the OR proofs algorithm (which proves that a result of re-encrypting v is one of V1, V2, ...,vL) which is used in this case may be obtained by enhancing the above illustrative algorithm.

[0078] Specifically, a similar voting scheme as the above voting scheme is used by defining an aspect of encrypting vote "i" (i represents the numbers from 1 to L) as all that encrypting vi = (1, G^(M^i)).

[0079] In the proving process 20, the vote generating center 10 proves that a result of re-encrypting vote "i" is included in voting data for each vote "i" to prove that the voting data supplied from the vote generating center 10 includes all votes "i".

[0080] Concretely, an example of the OR proofs algorithm which proves that a result of encrypting v is one of v1, v2, ...,and vL may be achieved as follows.

[0081] OR proofs algorithm (multi value version)

(which proves that a result of re-encrypting v = (x, y) is included in a set vi = (xi, yi) (i = 1, ...,L))

[0082] Herein, it is assumed that a proving device knows j and α (xj = x g α mod p, yj = y h α mod p). 1. The proving device randomly selects di and ri (i = 1, ..., L), and calculates the following equations.

$$ai = (xi/x)^{di} * g^{ri} \bmod p$$

$$bi = (yi/y)^{di} * h^{ri} \bmod p$$

2. The proving device calculates the following equation.

$$c = H(x, y, x1, y1, ..., xL, yL, a1, ..., aL, b1, ..., bL).$$

3. If the result of re-encrypting v is equal to vj, dj is replaced with c-Σdi (i is an attached number other than j) and rj is replaced with αd' + rj - αdj (d' is dj before it is replaced).

4. Thus replaced d1, ..., dL, r1, ..., rL are defined as proofs.

5. The verifying device recalculates the following equations based on the received d1, ...,dL, r1, ...,rL.

$$ai =(xi/x)^{di} * g^{ri} \bmod p$$

$$ai =(yi/y)^{di} * g^{ri} \bmod p$$

[0083] In the contents transferring process 28, to inform correctness of contents of voting data, a re-encrypting algorithm may be employed which proves that a result of re-encrypting each vote "i" is a specific vj using the above designated-verifier algorithm.

[0084] Further, the proving process 31 or the correspondence transferring process 33 also may employ the OR proofs algorithm (multi value version) or the re-encrypting algorithm which proves using the above designated-verifier.

[0085] Hereinafter, description is made about a secure receipt-free voting method according to a second preferred embodiment of the invention.

[0086] In the second embodiment of the invention, voting data are configured of an encrypted vote. Other choice for voting may be selected by selecting a conversion parameter and converting the voting data with the selected conversion parameter. The second embodiment of the invention is schematically the same as the first embodiment of the invention. Thus, explanation is focused about points different from the first embodiment of the invention with reference to Figs. 1 and 2.

[0087] Here, it is assumed that voting allowed to be chosen on a vote "1" or a vote "0". The voting data is also arranged to be composed of a random choice of the vote "1" or the vote "0" subjected to rearrangement and to be given to each of the vote selecting device 12 (i). Next, the vote generating center 10 publicly proves that the voting data is generated correctly.

[0088] This is performed by the proving process 20. Moreover, the process 20 secretly transfers to the vote selecting device 12(i) via anti-eavesdropping channel 16(i), contents of the voting data, that is which vote is included in the voting data. Simultaneously, the vote generating center 10 proves that the contents of the voting data is correct via the anti-eavesdropping channel 16(i). the transferring and proving are performed by the contents transferring process 28 as described later.

[0089] The vote selecting device 12(i) selects the voting data itself or opposite vote to the voting data using a secret message sent from the vote generating center 10 via the physically anti-eavesdropping channel 16(i). Votes which are selected by the vote selecting devices 12(1), 12(2),..., 12(1) are transferred to the vote counting center 15 via the bulletin board. All encrypted votes are accumulated at the vote counting center 15, a result of voting is determined by decrypting the accumulated cryptograms. Each of the vote generating center 10, the vote selecting center 12(i), and the vote counting center

15 includes a calculation device may be preferably implemented by a personal computer, but may be a workstation or the like.

[0090] Next, description is made about the data configuring process 26, the proving process 20, the contents transferring process 28, and details of information transferred in secret via the anti-eavesdropping channel 16.

[0091] The vote generating center 10 generates voting data consisting of vote "0" or vote "1" and transfers it to each vote selecting device 12(i) by performing the data configuring process 26. The center 10 performs data configuring process for each vote selecting device 12 (i) using independently selected random number. An aspect of voting using the vote "1" and the vote "0" is similar to the first embodiment of the invention.

[0092] Next, in the data configuring process 26, the vote generating center 10 selects v1 or v0 with probability of 1/2, re-encrypts the selected vote using a randomly selected random number ri1, and generates viA as the voting data.

[0093] The vote generating center 10 posts the voting data viA to the bulletin board. In the proving process 20, the vote generating center 10 proves that a result of re-encrypting the vote "1" is either viA or viA^(-1) to prove that the voting data viA is the correct vote "1" or the correct vote "0". Concretely, the OR proofs algorithm which proves that a result of re-encrypting v is either v1 or v2, similar to the algorithm used in the first embodiment of the invention may be used.

[0094] Next , description is made of the contents transferring process 28. The process transfers contents of the voting, that is, whether contents of viA is the vote "1" or the vote "0", to the vote selecting device 12(i) via the anti-eavesdropping channel 16. The fact that the correspondence is correct is proved by proving via a similar anti-eavesdropping channel 16 that a result of re-encrypting the vote "1" is viA or that a result of re-encrypting the vote "0" is viA. Further, the proving is performed using a designated-verifier proof with a public key of the vote selecting device 12(i). Concretely, a re-encrypting proofs algorithm which proves that a result of re-encrypting v is v' using the designated-verifier proofs algorithm, similar to the algorithm used in the first embodiment of the invention may be used.

[0095] The vote generating center transfers the contents of the voting data and designated-verifier proofs representing the correctness of the voting data to the vote selecting device 12(i) via the anti-eavesdropping channel 16 as described above.

[0096] The vote selecting device 12(i) verifies the correctness of the contents proofs algorithm in the verifying process 24. When the correctness is verified, the vote selecting device 12(i) performs the selecting process 25, and selects a vote reflecting voters will from the voting data in the bulletin board and the reverse of the voting data. The vote selecting device may select correctly, because the contents of the voting data are correctly transferred to the vote selecting device by the contents transferring process.

[0097] To improve the security of receipt-free properties, a conversion network 11 including a plurality of converting centers 11(1), 11(2), ..., 11(m) may be incorporated as shown in Figs. 3 and 4. The voting data which are generated by the vote generating center 10 and are transferred to the vote selecting device 12(i) passed through the conversion network 11 before the voting data arrive at the vote selecting device 12(i). In such a configuration, it is impossible to determine how the vote selecting device 12(i) makes a ballot for malicious people, as long as all of the converting centers and the vote generating center conspire together or anti-eavesdropping channels 17(1), 17(2),...,17(m) each of which resides between one of the converting center and one of the vote selecting device 12(i) are all eavesdropped.

[0098] Next, description is made about operations of the conversion network and the converting center. The converting center 11 (j) sends the result of converting process 30 (shown in Fig. 5) which converts voting data sent from the previous converting center 11 (j-1)(when j=1, it represents the vote generating center 10). The above operation is repeated until the last converting center 11 (m) sends its result. Each of the converting centers informs the vote selecting device of how the voting data are converted via secure anti-eavesdropping channel 17(j).

[0099] Each of the converting centers proves to the vote selecting device that the conversion is correctly performed and incorrect information is not provided, as similar to the vote generating center. This operation is performed by proving process 31 and correspondence proofs algorithm 33.

[0100] Fig. 5 shows an operation of the converting center 11(i). The converting center 11(i) performs the converting process 30 and the proving process 31, and sends its output. The proving process 31 publicly proves that conversion is correctly performed. The correspondence transferring process 32 proves how the actual conversion is performed and that information is not incorrect only to the vote selecting device with the designated-verifier correspondence proofs algorithm 33.

[0101] Next, description is made about the converting process 30. It is assumed that input data to the process are voting data V1.

[0102] The converting algorithm selects v1 or v1^(-1) with a probability of 1/2, re-encrypts the selected value with random number c, and sends the result as VA.

[0103] The proving process 31 is used to prove that the converting center correctly performs the converting algorithm. The proving process 31 includes a proving device and a verifying device. In this case, the proving device is the converting center. The verifying device may be any entity including the vote selecting device. This concretely means that it satisfies to prove that a result of re-encrypting V1 is either VA or VA^(-1) by using the above mentioned OR proofs algorithm.

[0104] Proving process may use any algorithm which may prove that given output voting data is a result of re-encrypting input voting data itself or reverse of the input voting data, without showing whether actual reverse is performed or not.

[0105] Next, description is made about correspondence transferring process 32. The process informs the vote selecting device 12(i) of whether V1 is re-encrypted or the reverse of V1 is re-encrypted. The correctness of the converting is proved by proving that a result of re-encrypting V1 is VA when V1 is re-encrypted and that a result of re-encrypting V1^(-1) is VA with designated-verifier proofs when the reverse of V1 is re-encrypted. This is achieved by using the designated-verifier re-encryption proofs algorithm.

[0106] The voting data sent from the vote generating center are sequentially processed by the converting centers 11(1), 11(2), ...,11(m) and these processes are repeated until the last converting center randomly and traceably converts the voting data and sends it to each vote selecting device. The vote selecting device 12(i) selects a vote via the secure anti-eavesdropping channels 16(i), 17(1), 17(2), ...,17(m) using secret messages received from the vote generating center and the converting center.

[0107] Invalidation of proving of that converting center is implemented similar to the invalidation of proving of the vote generating center.

[0108] Here, to simplify the description, a voting scheme which selects one from vote "0" and vote "1" is illustrated. However, in a voting scheme which selects one among more than three votes, an aspect of the embodiment may be adopted. Specifically, it is defined that a vote "i" (i represents the numbers from 1 to L) is represented as a vector having L elements each element taking 1 in i-th element and 0 in the other elements, for example, (0, ..., 0, 1, 0,..., 0). Also, an aspect of encrypting of the vector is defined as a result of re-encrypting (1, G) about the i-th element, or as a result of re-encrypting (1,1) about the other elements. By accumulating for each element, the number of votes selected by voters is recognized for each element in the same principle as mentioned above.

[0109] In such definition, to convert vote "i" to vote "j", (j - 1 mod L) times of cyclic shift operations are performed for all elements so that the i-th element is changed to the j-th element. In this case, each converting center performs predetermined number of times of shift operations for each element of the input voting data which form a vector having L values, and secretly informs the vote selecting device of the number of times of the shift operations.

[0110] The vote selecting device may select encrypted vote by selecting the number of shift operations for each element of L values of the voting data which may be converted to his/her own vote based on the final voting data.

[0111] In the proving process 20, the vote generating center 10 proves that predetermined number of times of shift operations for vote "1" represented as (1, 0, ...,0) leads to the generated voting data representing vote "i". This proving may be performed by using the above OR proofs algorithm in a two-dimensional manner.

[0112] The contents transferring process 28, to inform that the contents of the voting data are just the same as vote "i", proves that a result of re-encrypting vote "i" is the voting data for each element using re-encryption proofs algorithm which proves with the above designated-verifier.

[0113] Further, the proving process 31 or the correspondence transferring process 32 may use the above described OR proofs algorithm (two-dimensional version) or the re-encryption proofs algorithm in a plurality of times in the same way.

[0114] Some preferred embodiments of the invention have been described. Next, description is made about a preferred system configuration of the invention.

[0115] In Fig. 1, the system used to implement the first embodiment of the invention is shown. The system includes the vote generating center 10, the vote selecting devices 12(1), 12(2), ..., 12(1), and the vote counting center 15, each of which operates on a personal computer or a workstation connected to a previous type of bulletin board 13. The vote generating center 10 may transfer secret messages to each vote selecting device via secure anti-eavesdropping channels 16(1), 16 (2), ..., 16(1). All of the elements which perform message transferring processes including a sending section, a verifying device, and a center) send or receive messages via the bulletin board 13 or receive the messages between them with the exception of sending secret messages by the vote generating center to the vote selecting via the anti-eavesdropping channels. The vote generating center or the vote selecting device is also operable as the vote counting center. The personal computer may store a software which may performs the above method or may include the elements shown in Fig. 2 as a hardware or a software.

[0116] In Fig. 2, how messages are transferred for a receipt-free voting is shown. As described above, the vote generating center 10 generates voting data using the data configuration process 26 and sends the voting data to the vote selecting device 12(i). The vote generating center then performs the proving process 20. Outputs of the contents transferring process 28 and the contents proofs algorithm 22 which the correctness of the contents are sent to the vote selecting device 12(i) via the anti-eavesdropping channel 16(i). The other output from the vote generating center 10 are sent to the bulletin board 13. The vote selecting device 12(i) performs the verifying process 24 and the selecting process 25, and outputs encrypted votes selected by using voting data on the bulletin board. The encrypted votes selected by each of the vote selecting devices 12(1), 12(2), ...,12 (1) are transferred to the vote counting center 15 via the bulletin board.

[0117] In Fig. 3, a system of the second embodiment of the invention which uses a conversion network. The system includes the vote generating center 10, the converting centers 11(1), 11(2), ...,11(m), the vote selecting devices 12(1), 12(2), ..., 12(1), and the vote counting center 15, each of which operates on a personal computer or a workstation connected to a previous type of bulletin board 13. The vote generating center 10 may transfer secret messages to each vote selecting device via secure anti-eavesdropping channels 16(1), 16 (2), ..., 16(1). Further, the system includes the anti-eavesdropping channels 17(1), 17(2), ...17(m), and may transfer secret messages from the converting centers 11(1), 11(2), ...11(m) to the vote selecting device 12 (i) via the channels. All of the elements which perform a message transferring process (including a sending section, a verifying device, and a center) send or receive messages via the bulletin board 13 or receive the messages between them with the exception of sending secret messages by the vote generating center to the vote selecting device via the anti-eavesdropping channels. The vote generating center or the vote selecting device is also operable as the vote counting center or converting center. The personal computer may store a software which may performs the above method or may include the elements shown in Figs. 4 and 5 as a hardware or a software.

[0118] In Fig. 4, how messages are transferred for a receipt-free voting with the conversion network is shown. The vote generating center 10 generates voting data generates voting message for the vote selecting device 12(i) and sends the voting data to the bulletin board 13. Then, the converting center 11(1) reads the voting data from the bulletin board 13, performs the converting process 30 and the proving process 31, and sends the converted voting data to the bulletin board 13.

[0119] On the other hand, the converting center 11(1) sends secret messages which include outputs of the correspondence transferring process 32 and the correspondence proofs algorithm 33 which proves the correctness of the correspondence, to the selecting device 12(i) via the anti-eavesdropping channel 17(1). Similarly, the following converting centers reads the output of the previous center from the bulletin board 13 and sends its own output to the bulletin board to provide it to the next center. The converting centers 11(1) also send secret messages to the vote selecting device 12(i) via the anti-eavesdropping channel 17(1). The selecting device 12(i) reads the last converting center's output, performs the verifying process 35 and the selecting process 36, and sends the vote selected using the voting data on the bulletin board. The encrypted votes selected by each of the vote selecting devices 12(1), 12(2), ...,12(1) are transferred to the vote counting center 15 via the bulletin board.

[0120] After the vote generating center sends the secret messages, the vote selecting device 12(i) performs the invalidating process 37 and proves the validation of the center.

[0121] In Fig. 5, the converting center 11 (i) includes the converting process 30, the proving process 31, and the correspondence transferring process 32, and performs them. Further, the correspondence transferring process 32 uses the correspondence proofs algorithm 33.

[0122] While there has been described a secure receipt-free electronic voting method and system, it will be apparent to those skilled in the art that variations and modifications of the invention are possible within the disclosure and the scope of spirit defined by claims of the invention.

[0123] As described above, using the method and system of the invention, it is possible to provide a method of effectively realizing a secure receipt-free protocol with minimum physical limitation without supplying to a voter a receipt representing the contents of his/her voting action.

Claims

1. A receipt-free electronic voting method comprises the steps of:

   (a) generating voting data and posting them to a bulletin board;
   (b) sending a secret message to a vote selecting device without being monitored;
   (c) selecting, at the selecting device, a vote using the voting data on the bulletin board; and
   (d) counting, at a counting center, the votes.

2. The method of claim 1, wherein step (b) is performed via a secure anti-eavesdropping channel.

3. The method of claim 1 or 2 further comprising the step of proving the correctness of the voting data.

4. The method of claim 3, wherein the proving step also provides proofs assuring the correctness of the contents of the voting data.

5. The method of anyone of claims 1 to 4, wherein the secret message includes the contents of the voting data.

6. The method of anyone of claims 1 to 5, wherein the secret message includes at least part of proofs assuring the correctness of contents of the voting data.

7. The method of claims 4 or 6, wherein the proofs assuring the correctness of contents of the voting data are designated-verifier proofs in which the verifier is the vote selecting device.

8. The method of claim 7, wherein the vote selecting device provides invalidating of the proofs.

9. The method of claim 8, wherein the invalidating of the proofs is performed by providing a secret key of the vote selecting device to the bulletin board.

10. The method of anyone of claims 1 to 9, wherein step (a) further comprises the steps of:

(i) converting the generated voting data; and
(ii) sending the secret message relating to the conversion to the vote selecting device without being monitored.

11. The method of claim 10, wherein step (ii) is performed via a secure anti-eavesdropping channel.

12. The method of claim 10 or 11 further comprising the step of proving the correctness of the voting data.

13. The method of claim 12 wherein the proving step also provides proofs assuring the correctness of the contents of the converted voting data.

14. The method of anyone of claims 10 to 13, wherein the secret message includes the contents of the converted voting data.

15. The method of anyone of claims 10 to 14, wherein the secret message includes at least part of proofs assuring the correctness of contents of the converted voting data.

16. The method of claim 13 or 15, wherein the proofs assuring the correctness of contents of the converted voting data are designated-verifier proofs in which the verifier is the vote selecting device.

17. The method of claim 16, wherein the vote selecting device provides invalidating of the proofs.

18. The method of claim 17, wherein the invalidating of the proofs is performed by providing a secret key of the vote selecting device to the bulletin board.

19. A receipt-free electronic voting system comprising:

one or more vote generating centers (10);
a plurality of vote selecting devices (12(1)-(l));
a bulletin board (13); and
a vote counting center (15), wherein
the vote generating center (10) generates voting data, posts them to the bulletin board, and sends a secret message to each vote selecting device (12(1)-(l)) without being monitored, each of the vote selecting devices (12(1)-(l)) selects a vote using the voting data via the bulletin board (13), and the vote counting device (15) counts the votes.

20. The system of claim 19, wherein the vote generating center (10) sends the secret message to the vote selecting device (12(1)-(l)) via a secure anti-eavesdropping channel (16(1)-(l)).

21. The system of claims 19 or 20, wherein the vote generating center (10) proves the correctness of the voting data.

22. The system of anyone of claims 19 to 21, wherein the vote generating center (10) provides proofs assuring the correctness of the contents of the voting data.

23. The system of claim 21 or 22, wherein the vote selecting device (12(1)-(l)) provides invalidating of the proofs.

24. The system of anyone of claims 19 to 23, further comprising a conversion network (11) which receives the generated voting data and includes a plurality of converting centers (11(1)-(m), wherein each of the converting centers (11(1)-(m)) converts the voting data and sends the secret message to the vote selecting device (12(1)-(l)) without being monitored.

25. The system of claim 24, wherein each of the converting centers (11(1)-(m)) sends the secret message to the vote selecting device (12(1)-(l)) via a secure anti-eavesdropping channel (17(1)-(m)).

26. The system of claims 24 or 25, wherein each of the converting centers (11(1)-(m)) proves the correctness of the converted voting data.

27. The system of anyone of claims 24 to 26 , wherein each of the converting centers (11(1)-(m)) provides proofs assuring the correctness of the contents of the converted voting data.

28. A recording medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform a receiptfree electronic voting method, comprising the steps of:

(a) generating voting data and posting them to a bulletin board;
(b) sending a secret message to a vote selecting device without being monitored;
(c) selecting, at the selecting device, a vote using the voting data on the bulletin board; and
(d) counting, at a counting center, the votes.

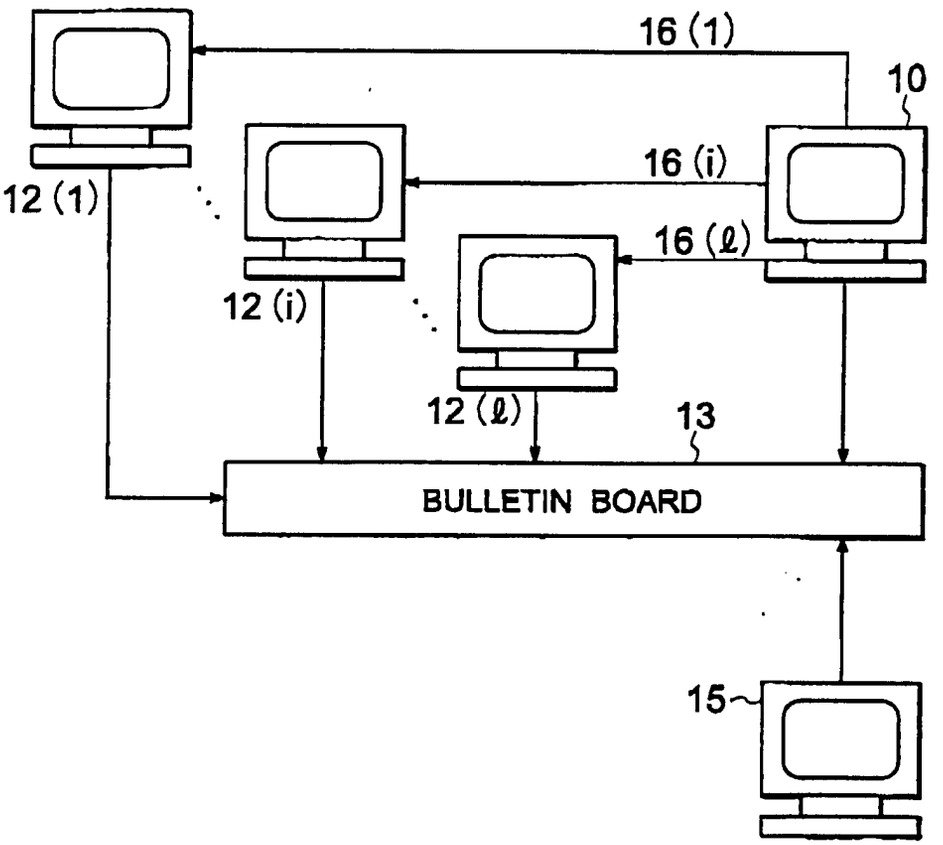

FIG. 1

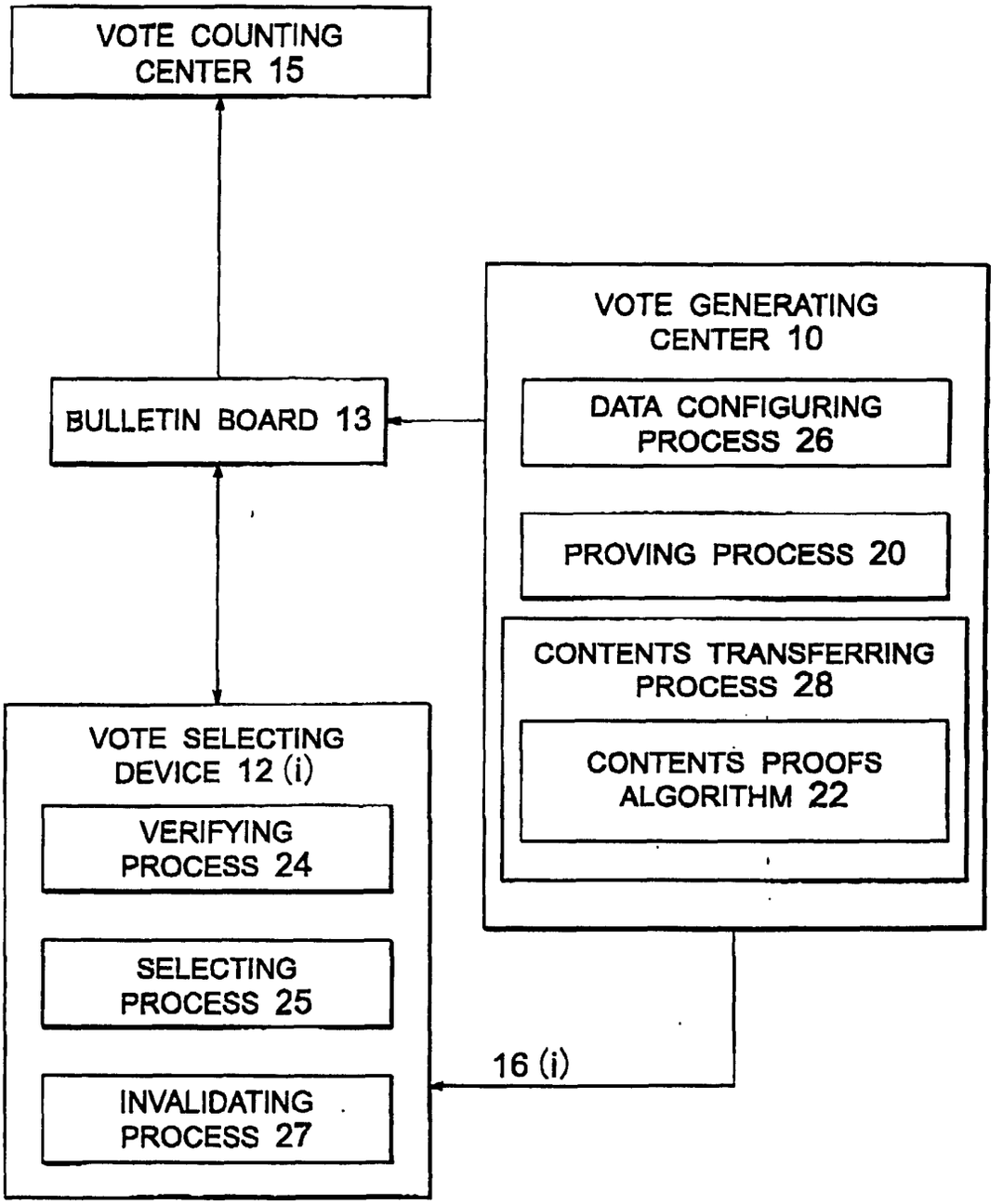
VOTE COUNTING CENTER 15
VOTE GENERATING CENTER 10
DATA CONFIGURING PROCESS 26
BULLETIN BOARD 13
PROVING PROCESS 20
CONTENTS TRANSFERRING PROCESS 28
CONTENTS PROOFS ALGORITHM 22
VOTE SELECTING DEVICE 12 (i)
VERIFYING PROCESS 24
SELECTING PROCESS 25
INVALIDATING PROCESS 27
16 (i)

FIG. 2

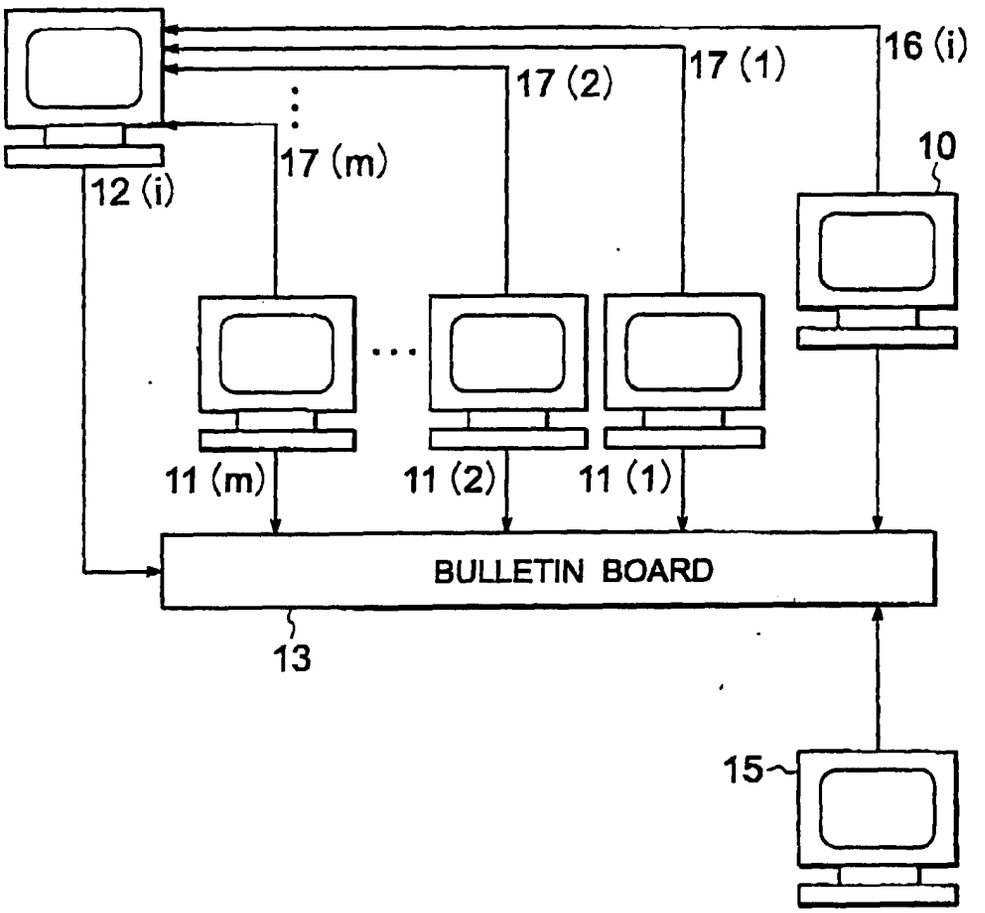

FIG. 3

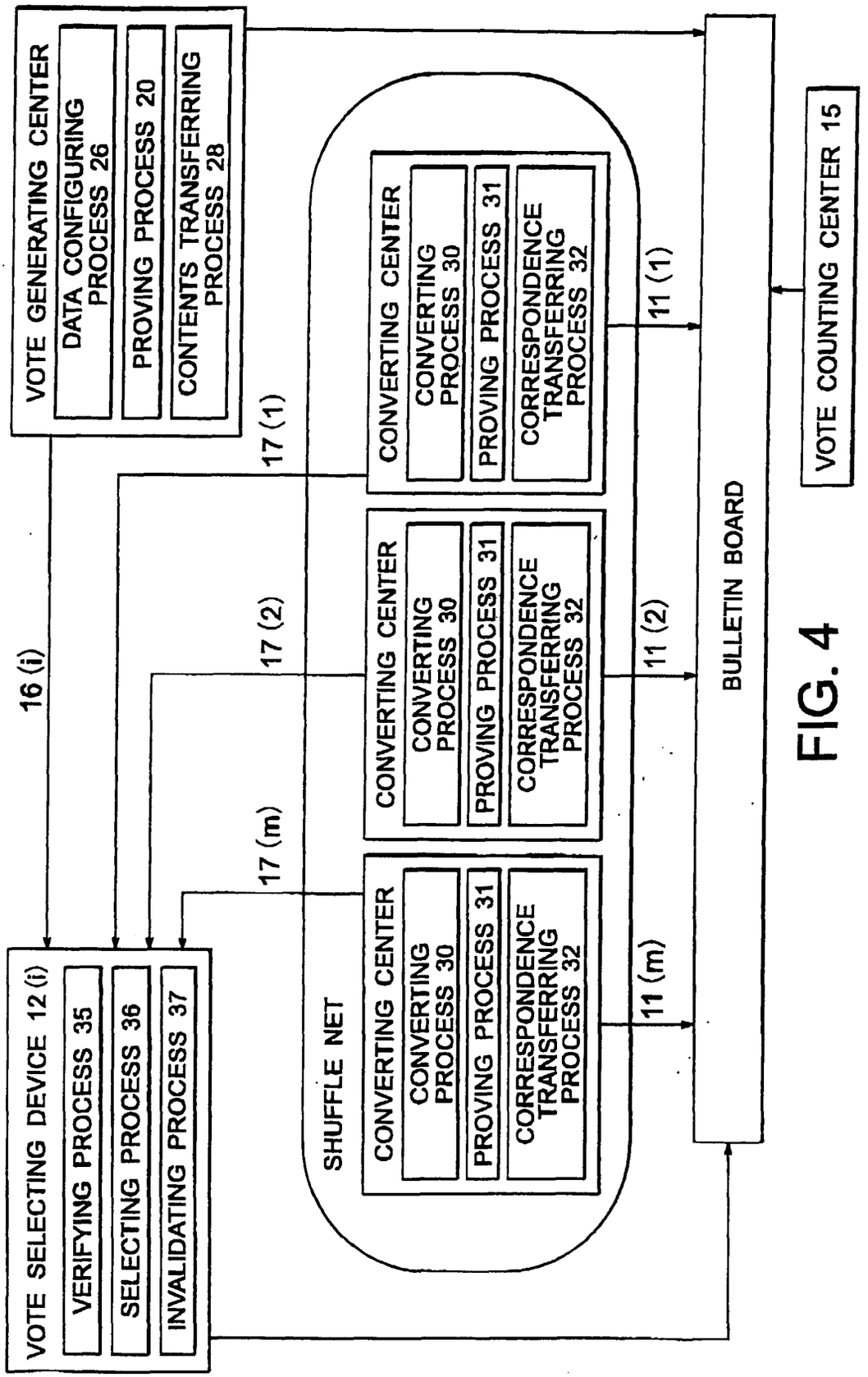
VOTE GENERATING CENTER
DATA CONFIGURING PROCESS 26
PROVING PROCESS 20
CONTENTS TRANSFERRING PROCESS 28
16 (i)
17 (1)
17 (2)
17 (m)
SHUFFLE NET
CONVERTING CENTER
CONVERTING PROCESS 30
PROVING PROCESS 31
CORRESPONDENCE TRANSFERRING PROCESS 32
CONVERTING CENTER
CONVERTING PROCESS 30
PROVING PROCESS 31
CORRESPONDENCE TRANSFERRING PROCESS 32
CONVERTING CENTER
CONVERTING PROCESS 30
PROVING PROCESS 31
CORRESPONDENCE TRANSFERRING PROCESS 32
11 (1)
11 (2)
11 (m)
BULLETIN BOARD
VOTE COUNTING CENTER 15
VOTE SELECTING DEVICE 12 (i)
VERIFYING PROCESS 35
SELECTING PROCESS 36
INVALIDATING PROCESS 37

FIG. 4

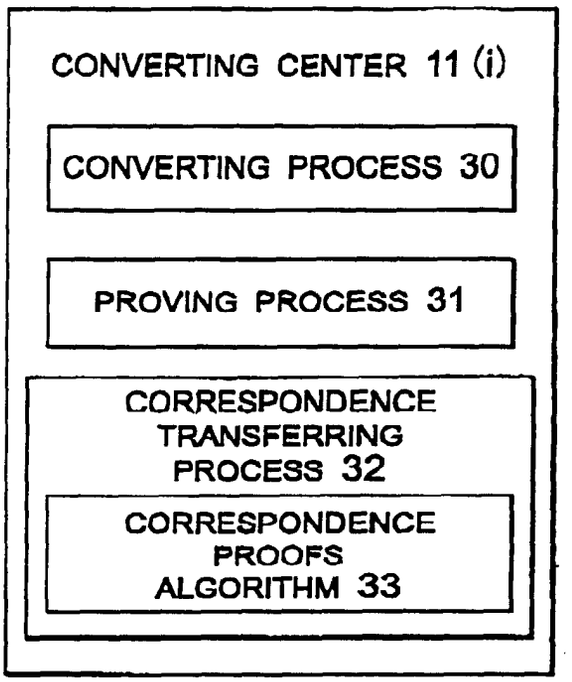
CONVERTING CENTER 11 (i)
CONVERTING PROCESS 30
PROVING PROCESS 31
CORRESPONDENCE TRANSFERRING PROCESS 32
CORRESPONDENCE PROOFS ALGORITHM 33

FIG. 5