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

(11) EP 2 382 606 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
13.02.2019 Bulletin 2019/07

(21) Application number: **08875902.2**

(22) Date of filing: **23.12.2008**

(51) Int Cl.:
G07C 13/00 $^{(2006.01)}$

(86) International application number:
PCT/IB2008/055521

(87) International publication number:
WO 2010/073065 (01.07.2010 Gazette 2010/26)

(54) **VERIFIABLE ELECTRONIC VOTING METHOD**
VERIFIZIERBARES ELEKTRONISCHES WÄHLVERFAHREN
PROCÉDÉ DE VÉRIFICATION D'UN VOTE ÉLECTRONIQUE

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

(43) Date of publication of application:
02.11.2011 Bulletin 2011/44

(73) Proprietor: **Tubitak**
06100 Ankara (TR)

(72) Inventor: **TIRYAKIOGLU, Fatih**
41470 Kocaeli (TR)

(56) References cited:

EP-A- 1 783 696	**FR-A- 2 895 552**
US-A1- 2005 035 199	**US-A1- 2007 187 498**
US-A1- 2008 135 632	**US-B1- 6 457 643**

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND

[0001] It is difficult to provide transparency and anonymity in electronic voting systems. Using paper trails for verification seems to be like paper based classic voting method and it does not solve verification problem completely. Such voting systems are disclosed in prior art document US 2008/0135632 A1. Voters want transparent electronic voting systems. But this should not result in vote buying. Electronic voting methods should be also user friendly and easy to understand. Secure, transparent, voter verifiable and anonymity based electronic voting methods are required for future electronic voting systems.

BRIEF DESCRIPTION OF INVENTION

[0002] The present invention defined in the method of independent claim 1, allows a voter to verify that the votes she cast were properly counted while maintaining vote anonymity. Anonymity and transparency are balanced such that voters have proofs showing the votes they cast are properly counted, but the same proofs are meaningless to the others. In this way, transparency is succeeded without exposing voter privacy. While voters cast their votes, for example in a voting machine, a witness is required to verify that the vote is counted properly. A witness proving voter privacy is implemented by using a voter superiority over the voting system. This strength is used to solve transparency-anonymity problem: Voting system can't guess next step of the voter, and when all steps are revealed, it is not allowed the system to get back. Voters present a random choice from a predetermined set of random choices together with each voting choice in the voting process, and she expects an algorithm output as a proof of including voting choices and random choices of the voting choices. After receiving algorithm output, she presents all random choices of each possible choice, and gets the random choices from the voting system as she presents. Because the voting system can not know random choices of the other possible choices, a possible malware code in the system can not dare to change voting choices of the voter. If it dares and the random choices of the not intended voting choices it selects is not as the random choices of the not intended voting choice entered following to receiving the algorithm output by the voter, then this illegal modification is revealed. The possibility of reveal increases exponentially, as the voting system's illegal modified votes increase. Algorithm output is an output of a cryptographic algorithm getting inputs that comprises voting choices and random choices of the voting choices and using a secret. The voting choices of the voters can't be computed by using the algorithm output without knowing the secret. The secret can be an input text, the algorithm, key, or a combination of them. Key is preferably used as a secret because of its strength against brute-force attacks.

[0003] Algorithm output and random choices of possible choices got by voter during the vote casting are also made public for future verification. Voter compares her algorithm output and random choices of possible choices with the ones made public, and if they are same she ensures for proper counting of her vote. Voting center verifies and evaluates the votes by using public parameters that comprise algorithm output and random choices of possible choices and secret. Illegal processes are revealed by the voting center, if any. Beside the voting center, a trusted third party that gets secrets from the voting center can be used for verification of the voting results.

BRIEF DESCRIPTION OF DRAWINGS

[0004]

FIG. **1** depicts a block diagram of a voting system that can implement the voting method.

FIG. **2** depicts the flowchart of the voting method.

FIG. **3** depicts a user interface on which a voter may enter voting choices and the random choices of the voting choices.

FIG. **4** depicts an optic paper that may be used for entering random choices of all possible choices to the voting system.

FIG. **5** depicts a paper that may be received by the voter for voter verification.

FIG. **6** depicts a look-up table on the voting machine that comprises verification texts of the voters.

DETAILED DESCRIPTION

[0005] The present invention allows a voter to verify that the votes she cast were properly counted while maintaining vote anonymity. The system 5 may be implemented as shown in FIG. **1.** The system **5** includes voting machines **10** which are located in voting precincts. While there are three voting machines in the FIG. **1,** any number of voting machines can be provided. Each voting machine comprises a human-machine interface **15,** a processing unit **20,** local databases **25** and **30.** Human-machine interface **15** provides communication and data transfer with the environment. Processing unit **20** is generally responsible for running electronic voting method and specifically runs an algorithm which uses secret S. Local database **25** holds verification texts of voters. Local database **30** holds candidate information which will be displayed in the human-machine interface. Prior to polls, candidate information is loaded to each local database **30** of the voting machines **10** separately from a central database **40** of voting center **35** by a central authority.

[0006] FIG. **2** is a flowchart showing the electronic voting method. The method may be implemented in a system **5** shown in the FIG. **1.** The method begins at step **100.** A voter is authorized to cast vote in a voting machine **10.** In step **105,** voter faces a user interface for selecting voting choices in the human-machine interface **15.** The user interface may be implemented as **300** shown in the FIG. **3.** In the user interface **300,** all candidates or choices **310** are presented. Each candidate or choice has a set of random choices **320** whose number and names are determined by a voting authority. Not later than step **120,** preferably prior to voting process for convenience, voter must have determined random choices of each candidate or choice except random choices of the voting choices. Random choices of the voting choices must have been determined up to this step. Random choice determination of the voter may be performed on a paper 400 like in the FIG. **4.** In the FIG. **4,** the choices **410** are shown in the first column, and the random choices **420** of the choices **410** are shown in rows for each choice. The voter's random choices in the FIG. **4.,** for example, are red, green, green, red, blue, green for mayor choice, and green, blue for yes/no choice, respectively. In the user interface **300** in the FIG. **3,** voter selects voting choices together with random choices of the voting choices which are determined prior to that. For example, if she chooses "Mehmet Camlibel" and "Yes" as shown in the FIG. **3,** she also enters "green" for "Mehmet Camlibel" and "green" for "Yes" due to prior determination shown in the FIG. **4.** Following the selection of voting choices and random choices of them, she casts vote. Vote casting may be implemented by a Cast button as shown in FIG. **3.** In step **110,** voting machine, receiving voter's voting choices and random choices of the voter's voting choices, processes a cryptographic algorithm using a secret.

[0007] Algorithm's input comprises voter's voting choices and random choices of the voter's voting choices and the algorithm produces output. The number of process/processes may be one or more than one. For example, there may be one process receiving "Mehmet Çamlibel", "green", "Yes", "green" or two processes, one of them receiving "Mehmet Camlibel", "green" and the other receiving "Yes", "green", etc. The processes, being more than one, may be independent or cascaded to each other as one's output is inputted to the other. In all conditions, it is guaranteed to input all voting choices and random choices of the voting choices and to receive output independent of the number of the process/processes and the output/outputs. The point here is that, all voting choices and random choices of the voting choices should be able to be guessed or determined by using algorithm output/outputs and the other known input parameters if the secret is known. Beside these, voting choices and random choices can be symbolized with different elements when inputting to the algorithm. For example, enumeration of the voting choices and the random choices can be performed. But the rule of the substitution must be public.

[0008] Algorithm's input can include an id determined by voter, voting machine, or both of them if a user friendly verification process is desired in the verification step. Algorithm's input may also include voting machine id which assures varying algorithm outputs across voting machines. Algorithm's input may include any optional data as long as voter's voting choices and random choices of the voter's voting choices are assured to be in the input parameters.

[0009] The algorithm makes use of a secret in the processing. The secret may be a key, a text inputted to the algorithm or the algorithm itself. It is preferably a key because of its strength against brute-force attacks trying to determine voting choices by using algorithm output/outputs and the other known input parameters. The point is that voting choices and random choices of the voting choices can't be determined by using only algorithm, algorithm outputs and the other known parameters, but also a secret is required.

[0010] In step **115,** the voter receives algorithm output and she makes sure it to be not changed in coming steps. After receiving algorithm output/outputs, but not before that, in step **120,** the voter enters all random choices of all possible choices to the voting system. This entrance may be performed by entering an optical paper **400** in FIG. **4** to an optic scanner of the voting machine. Then, in step **125,** the voter receives random choices of all possible choices just entered. This receiving together with the algorithm output, received in step **115,** can be named verification text of the voter. The verification text and the other optional parameters is given to the voter for future verification by the voter. They may be given to the voter on a paper **500** in FIG. **5.** In the FIG. **5,** the algorithm output **510,** the random choices **520** together with optional parameters, which are voter id **530** and voting machine id **540,** are shown. In step **130,** the voter compares entered and received random choices. In step **135,** she approves the voting if they are the same. If they are not the same, she rejects the voting and voting process ends with failure. The voter informs the officer for the incompatibility by showing her receiving. In step **140,** if approving realizes, all receiving are recorded to the local database of the voting machine, and vote casting for the voter ends with success. The voter also gets all receiving which may be like paper **500** in FIG. **5.** Beside these, in step **120,** if the random choices of the voting choices are entered again, which is usual in the optical paper implementation, the voting process may be ended with failure or may continue in normal flow depending on the voting authority's decision on method implementation. If the method is implemented as the voting process to end with failure, when the incompatibility happens in step **120,** i.e. the random choices of the voting choices entered in the user interface **300** in FIG. **3** in step **105** does not fit into the random choices of the voting choices on the paper **400** in FIG. **4** in step **120,** the vote casting ends with failure. If the method is implemented as the voting process to continue, when the incompatibility happens in step

120, i.e. the random choices of the voting choices entered in the user interface **300** in FIG. **3** in step **105** does not fit into the random choices of the voting choices on the paper **400** in FIG. **4** in step **120,** voting interface warns the voter for this incompatibility. If the voter accepts the incompatibility, the vote casting may be still valid, but there must be a sign of incompatibility, but not in detail as which one does not fit to which one, in the verification text which is received by the voter and stored in local database. If she does not accept the incompatibility, the vote casting ends with failure. In failure, all voting process must start from very beginning because of the disclosure of the random choices.

[0011] This process is repeated for all voters during the polls. After the polls are closed, verification texts and the other optional parameters of all voters are in the local database **25** in FIG. **1.** The local database may be implemented as the table **600** shown in FIG. **6.** In the FIG. **6,** each row **610** contains information related to one voter. The sequence of the voters is preferably random, and the table preferably does not contain voting time and additional information threating voter anonymity if maximum degree of vote-voter anonymity is required.

[0012] After the polls are closed, the data on the local databases of the voting machines is transferred to the central database **40** of the voting center **35** in FIG. **1.** Transferring of the information can be on-line or off-line. For enhanced security, the data is preferably copied from the local database to a storage in off-line, then the data can be transferred to the voting center in on-line. This ensures of not getting out any intentional or non-intentional information that will threaten vote anonymity from the voting machine. Making public of database on each voting machine can be performed by each voting machine locally, by the voting center globally after the transfer, or both locally and globally.

[0013] Evaluation and declaration of results can be performed by the voting center globally, or by both the voting center globally and each voting machine locally. Evaluation here means determining all voting choices from each voting machine's database which comprises algorithm outputs, random choices of all candidates/choices, and the other known parameters of each voter by using the secret of each voting machine. For the evaluation, the secret is required. The voting machine may also count votes simply during the polls, and the counts may be used in the local declaration without evaluation of the results. However these results are not basic, but evaluation of results by the voting center is required for certain results. The stored data and the voting results of each voting machine are made public globally by the voting center or globally by the voting center and locally by each voting machine after the polling is closed. The declaration of the stored data and the results of each voting machine is visualized in FIG. **1.**

[0014] The secrets of the algorithms can be generated in the voting machines locally, or they can be generated in voting center, and distributed to each voting machine. In the later case, the secrets are stored in voting center. If the secrets are generated in the voting machines, they are transferred to the voting center prior to evaluation of results. But the confidentiality of the secrets must be guaranteed during the transfer. Voting machines do not expose the secrets, they preferably zeroize the secrets after the polls are closed and the confidentiality of the secrets is realized for the transfer if transfer is required.

[0015] After the polls are closed, the data collected from the local databases is made public. Each voter finds her receiving got from voting machines during the voting process from the data made public. If she finds the receiving as is, she can make sure of proper counting of her vote. On the other hand, voting center evaluates votes and verifies the proper casting of votes by using data collected from the databases of voting machines. Beside these, a trusted third party can repeat the verification and evaluation of votes by using the secrets received confidentially from the voting center. And finally, the secrets of some or all voting machines may be disclosed for public evaluation and verification of votes. The verifications, verification and evaluation by the voting center, verification by the voters and verification by a trusted third party are shown in FIG. **1.**

Claims

1. An electronic voting method comprising:

a. Receiving a voting choice related to a supported candidate and a random choice from a set of predetermined random choices, the received random choice being assigned to the received candidate choice, namely the voting choice, via a human-machine interface of a voting machine,

b. generating an output of a cryptographic algorithm for performing encryption by the voting machine, wherein

the cryptographic algorithm makes use of a secret,

the inputs to the cryptographic algorithm comprising the voting choice and the random choice

c. Printing the algorithm output on a paper receipt,

d. Receiving a random choice for each candidate from the set of predetermined random choices assigned to each of the candidates via an optic scanner of the voting machine,

e. Printing all of the random choices received in step (d) on the paper receipt,

f. Waiting until the received random choices of step (d) are compared with the printed random choices of step (e) by a voter,

g. Receiving approval of the voter if the received and printed random choices are the same or,

h. Receiving rejection by the voter if the received and printed random choices are not the same and informing an officer of the incompatibility,

i. if approved, storing data comprising a voter's verification text that is comprised of the algorithm output of step (b) and the random choices of step (d) in a local database of the voting machine, and providing the paper receipt to the voter,

j. after the polls are closed, transferring the data on the local databases of the voting machines to a central database of a voting center and making the transferred data public,

k. checking proper counting of the votes when the voters check their verification texts with the data made public,

l. assuring proper counting of the votes by the voting center by verifying the proper casting of votes during evaluation of votes from the data collected from the databases of voting machines by using the stored data comprising the algorithm output, the random choices of step (d) and the secret of each voting machine on which a vote is cast.

2. The electronic voting method according to claim 1, wherein if firstly entered random choice related to the voting choice in step (a) and lastly entered random choice related to the voting choice in step (d) are not the same, the voting process ends with failure or continues in normal flow depending on the voting authority's decision on method implementation.

3. The electronic voting method according to claim 1, wherein the voting method is performed in all voting machines.

4. The electronic voting method according to claim 1, wherein if a possible malware code in the system dares to change the voting choice of the voter, illegal modification/malware is revealed provided that when the voter enters random choices related to all possible candidate choices and if the random choice entered by the voter as to malware-related candidate choice is not same as the random choice chosen by the malware code and taken as an input for the cryptographic algorithm to produce algorithm output in the prior step to entering random choices related to all possible choices by the voter.

5. The electronic voting method according to claim 1, wherein a trusted third party can perform the evaluation and verification of votes in the same way the voting center does by using the data stored in the voting machines containing information as to algorithm output and random choices of all possible choices peculiar to each voter as well as the secrets of the voting machines received confidentially from the voting center.

6. The electronic voting method according to claim 5, wherein the voting results obtained in each of the voting machines through the verification of votes performed by both the voting center and the trusted third party are respectively compared with each other in order to ensure that the voting center and the trusted third party arrive at the same voting results in the same voting machines.

7. The electronic voting method according to claim 1, wherein the evaluation and verification of votes can be publicly performed on some or all of the voting machines provided that the secrets of these voting machines are made public by the voting center, and the secrets coupled with the data stored in the voting machines comprising the algorithm output and random choices of all possible choices are used for the verification of votes.

Patentansprüche

1. Eine elektronische Wahlmethode, die Folgendes umfasst:

a. Den Erhalt einer auf einen unterstützten Kandidaten bezogenen Wahlentscheidung und eine zufällige Auswahl aus einer Menge von vorbestimmten zufälligen Auswahlen und die empfangene zufällige Auswahl wird der erhaltenen Stimme für den Kandidaten, nämlich der Wahlentscheidung, über eine Mensch-Maschinen-Schnittstelle oder ein Wahlgerät zugeordnet,

b. die Erzeugung einer Ausgabe eines kryptografischen Algorithmus für die Durchführung einer Verschlüsselung durch das Wahlgerät, worin

der kryptografische Algorithmus ein Geheimnis nutzt,

die Eingaben in den kryptografischen Algorithmus die Wahlentscheidung und die zufällige Auswahl umfassen,

c. den Druck der Algorithmus-Aufgabe auf einen Papierbeleg,

d. den Empfang einer zufälligen Auswahl für jeden Kandidaten aus der Menge vorbestimmter zufälliger Auswahlen, die jedem der Kandidaten über einen optischen Scanner des Wahlgeräts zugeordnet sind,

e. den Druck aller zufälligen Entscheidungen, die in Schritt (d) auf dem Papierbeleg empfangen werden,

f. das Warten, bis die erhaltenen zufälligen Auswahlen von Schritt (d) mit den gedruckten zufälligen Auswahlen von Schritt (e) durch einen Wähler verglichen werden,

g. den Erhalt der Zustimmung des Wählers, wenn die erhaltenen und gedruckten zufälligen

Auswahlen übereinstimmen, oder

h. den Erhalt der Zurückweisung durch den Wähler, wenn die erhaltenen und gedruckten Auswahlen nicht übereinstimmen und die Information eines Verantwortlichen über die Inkompatibilität,

i. wenn die Zustimmung erhalten wird, die Speicherung der Daten, welche den Überprüfungstext eines Wählers umfassen, der aus der Algorithmus-Ausgabe von Schritt (b) und den zufälligen Auswahlen von Schritt (d) in einer lokalen Datenbank des Wahlgeräts umfassen und dem Wähler den Papierbeleg bereitstellen,

j. nachdem die Wahllokale geschlossen sind, die Übertragung der Daten der lokalen Datenbanken des Wahlgeräts an eine zentrale Datenbank eines Wahlzentrums und die Veröffentlichung der übertragenen Daten,

k. die Überprüfung der richtige Zählung der Stimmen, wenn die Wähler ihre Überprüfungsstexte mit den veröffentlichten Daten kontrollieren,

l. die richtige Zählung der Stimmen durch das Wahlzentrum sicherzustellen, indem die richtige Abgabe der Stimmen während der Evaluierung der Stimmen aus den von den Datenbanken der Wahlgeräte gesammelten Stimmen verifiziert wird, indem die gespeicherten Daten, welche die Algorithmus-Ausgabe, die zufälligen Entscheidungen von Schritt (d) und das Geheimnis jedes Wahlgeräts, an dem eine Stimme abgegeben wird, umfassen, verwendet werden.

2. Die elektronische Wahlmethode gemäß Anspruch 1, worin, wenn die zuerst eingegebene zufällige Auswahl hinsichtlich der Wahlentscheidung in Schritt (a) und die zuletzt eingegebene zufällige Auswahl hinsichtlich der Wahlentscheidung in Schritt (d) nicht übereinstimmen, der Wahlvorgang abhängig von der Entscheidung der Wahlbehörde über die Methodenimplementierung mit einem Fehler endet oder sich sein normaler Ablauf fortsetzt.

3. Die elektronische Wahlmethode gemäß Anspruch 1, worin die Wahlmethode in allen Wählgeräten durchgeführt wird.

4. Die elektronische Wahlmethode gemäß Anspruch 1, worin, wenn ein möglicher Schadcode im System die Wahlentscheidung des Wählers ändert, die illegale Modifikation/Schadsoftware enthüllt wird, vorausgesetzt, dass wenn der Wähler zufällige Auswahlen hinsichtlich aller möglichen Kandidatenentscheidungen eingibt und die zufälligen Auswahlen durch den Wähler im Vergleich zur zufälligen Auswahl durch den Schadsoftwarecode nicht identisch sind und als Eingabe für den kryptografischen Algorithmus verwendet werden, um im vorherigen Schritt der Eingabe zufälliger Auswahlen hinsichtlich aller möglichen Kandidatenentscheidungen durch den Wähler Algorithmus-Ausgaben zu erzeugen.

5. Die elektronische Wahlmethode gemäß Schritt 1, worin ein vertrauenswürdiger Dritter die Evaluierung und Verifizierung auf die gleiche Art und Weise wie das Wahlzentrum durchführen kann, indem er die in den Wahlgeräten gespeicherten Informationen für die Algorithmus-Ausgabe und die zufälligen Auswahlen aller möglichen Auswahlen, die jedem Wähler eigen sind, ebenso wie die Geheimnisse der Wählgeräte, die er vertraulich vom Wahlzentrum bekommen hat, verwendet.

6. Die elektronische Wahlmethode gemäß Anspruch 5, worin die in jedem der Wahlgeräte durch die Verifizierung der Stimmen, die sowohl vom Wahlzentrum als auch den vertrauenswürdigen Dritten jeweils ausgeführt werden, erhaltenen Ergebnisse miteinander verglichen werden, um sicherzustellen, dass das Wahlzentrum und der vertrauenswürdige Dritte in denselben Wahlgeräten zu denselben Wahlergebnissen kommen.

7. Die elektronische Wahlmethode gemäß Anspruch 1, worin die Evaluierung und Verifizierung der Stimmen öffentlich an einigen oder allen der Wahlgeräte durchgeführt werden kann, vorausgesetzt, das die Geheimnisse dieser Wahlgeräte vom Wahlzentrum veröffentlicht werden, und die mit den in den Wahlgeräten gekoppelten Geheimnisse, welche die Algorithmus-Ausgabe und die zufälligen Auswahlen aller möglichen Auswahlen umfassen, zur Verifizierung der Stimmen verwendet werden.

Revendications

1. Un procédé de vote électronique comprenant :

a. La réception d’un choix de vote lié à un candidat soutenu et un choix aléatoire parmi un ensemble de choix aléatoires prédéterminés, le choix aléatoire reçu étant attribué au choix de candidat reçu, notamment le choix de vote, via une interface homme-machine d’une machine de vote,

b. Générer une sortie d’un algorithme cryptographique pour effectuer un cryptage par la machine à voter, dans laquelle

- l’algorithme cryptographique utilise un secret,
- les entrées de l’algorithme cryptographique comprenant le choix de vote et le choix aléatoire

c. Imprimer l'algorithme de sortie sur un reçu papier,

d. Recevoir un choix aléatoire pour chaque candidat parmi l'ensemble de choix aléatoires prédéterminés attribués à chacun des candidats via un scanner optique de la machine de vote,

e. Imprimer tous les choix aléatoires reçus à l'étape (d) sur le reçu en papier,

f. Attendre jusqu'à ce que les choix aléatoires reçus de l'étape (d) soient comparés aux choix aléatoires imprimés de l'étape (e) par un électeur,

g. Recevoir l'approbation de l'électeur si les choix aléatoires reçus et imprimés sont identiques ou,

h. Recevoir le rejet par l'électeur si les choix aléatoires reçus et imprimés ne sont pas identiques et informer un officier de cette incompatibilité,

i. Si l'approbation est reçue, stocker des données comprenant le texte de vérification de l'électeur composé de l'algorithme de sortie de l'étape (b) et des choix aléatoires de l'étape (d) dans une base de données locale de la machine de vote, et fournir le reçu papier à l'électeur,

j. Après la fermeture des bureaux de vote, transférer les données des bases de données locales des machines de vote vers une base de données centrale d'un centre de vote et rendre publiques les données transférées,

k. Vérifier le décompte des votes lorsque les électeurs vérifient leurs textes de vérification avec les données rendues publiques,

l. Assurer le comptage correct des votes par le centre de vote en vérifiant que les opérations de vote sont corrects lors de l'évaluation des votes à partir des données collectées des bases de données des machines de vote en utilisant les données stockées comprenant l'algorithme de sortie, les choix aléatoires de l'étape (d) et le secret de chaque machine de vote sur laquelle un vote est exprimé.

2. Le procédé de vote électronique selon la revendication 1, dans lequel le choix du vote en premier effectué en fonction du choix aléatoire de l'étape (a) et en dernier en fonction du choix du vote aléatoire de l'étape (d) sont différents, le processus de vote se termine par un échec ou se poursuit normalement, en fonction de la décision de l'autorité de vote sur la mise en oeuvre de la méthode.

3. Le procédé de vote électronique selon la revendication 1, dans lequel la méthode de vote est exécutée dans toutes les machines de vote.

4. Le procédé de vote électronique selon la revendication 1, dans lequel un code potentiel de maliciel (nuisible) dans le système ose changer le choix de vote de l'électeur, une modification illégale/un maliciel est révélé à condition que lorsque l'électeur entre des choix aléatoires liés à tous les choix de candidats possibles et si le choix aléatoire entré par l'électeur par rapport au choix de candidat lié au maliciel n'est pas identique au choix aléatoire choisi par le code du maliciel et utilisé comme entrée pour que l'algorithme cryptographique pour produire un algorithme de sortie à l'étape précédente pour faire entrer des choix aléatoires liés à tous les choix possibles par l'électeur.

5. Le procédé de vote électronique selon la revendication 1, dans lequel un tiers de confiance peut effectuer l'évaluation et la vérification des votes de la même manière que le centre de vote en utilisant les données stockées dans les machines de vote contenant des informations sur l'algorithme de sorite et des choix aléatoires de tous les choix possibles propres à chaque électeur, ainsi que les secrets des machines de vote reçus confidentiellement du centre de vote.

6. Procédé de vote électronique selon la revendication 5, dans lequel les résultats de vote obtenus dans chacune des machines de vote par la vérification des votes effectuée à la fois par le centre de vote et le tiers de confiance sont comparés les uns aux autres, afin de garantir que le centre de vote et le tiers de confiance parviennent aux mêmes résultats de vote dans les mêmes machines de vote.

7. Le procédé de vote électronique selon la revendication 1, dans lequel l'évaluation et la vérification des votes peuvent être effectuées publiquement sur une partie ou sur la totalité des machines de vote, à condition que les secrets de ces machines de vote soient rendus publics par le centre de vote et que les secrets soient accompagnés des données stockées dans les machines de vote comprenant l'algorithme de sortie et des choix aléatoires de tous les choix possibles sont utilisés pour la vérification des votes.

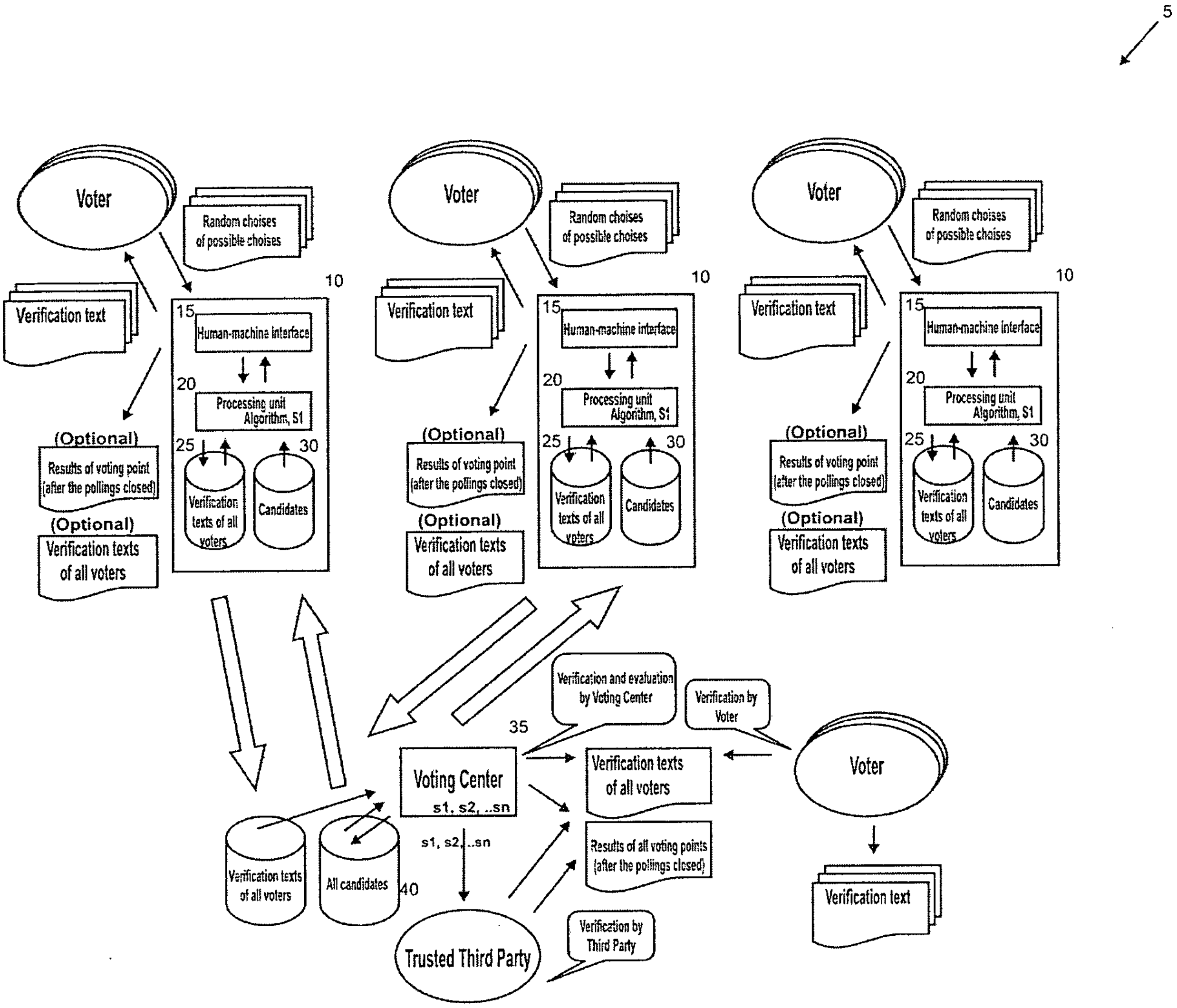

5
Voter
Random choises of possible choises
Verification text
10
15
Human-machine interface
20
Processing unit Algorithm, S1
25
30
Verification texts of all voters
Candidates
(Optional)
Results of voting point (after the pollings closed)
(Optional)
Verification texts of all voters
Verification and evaluation by Voting Center
Verification by Voter
35
Voting Center s1, s2, ..sn
s1, s2, ..sn
Verification texts of all voters
Results of all voting points (after the pollings closed)
All candidates
40
Trusted Third Party
Verification by Third Party
Voter
Verification text

FIGURE 1

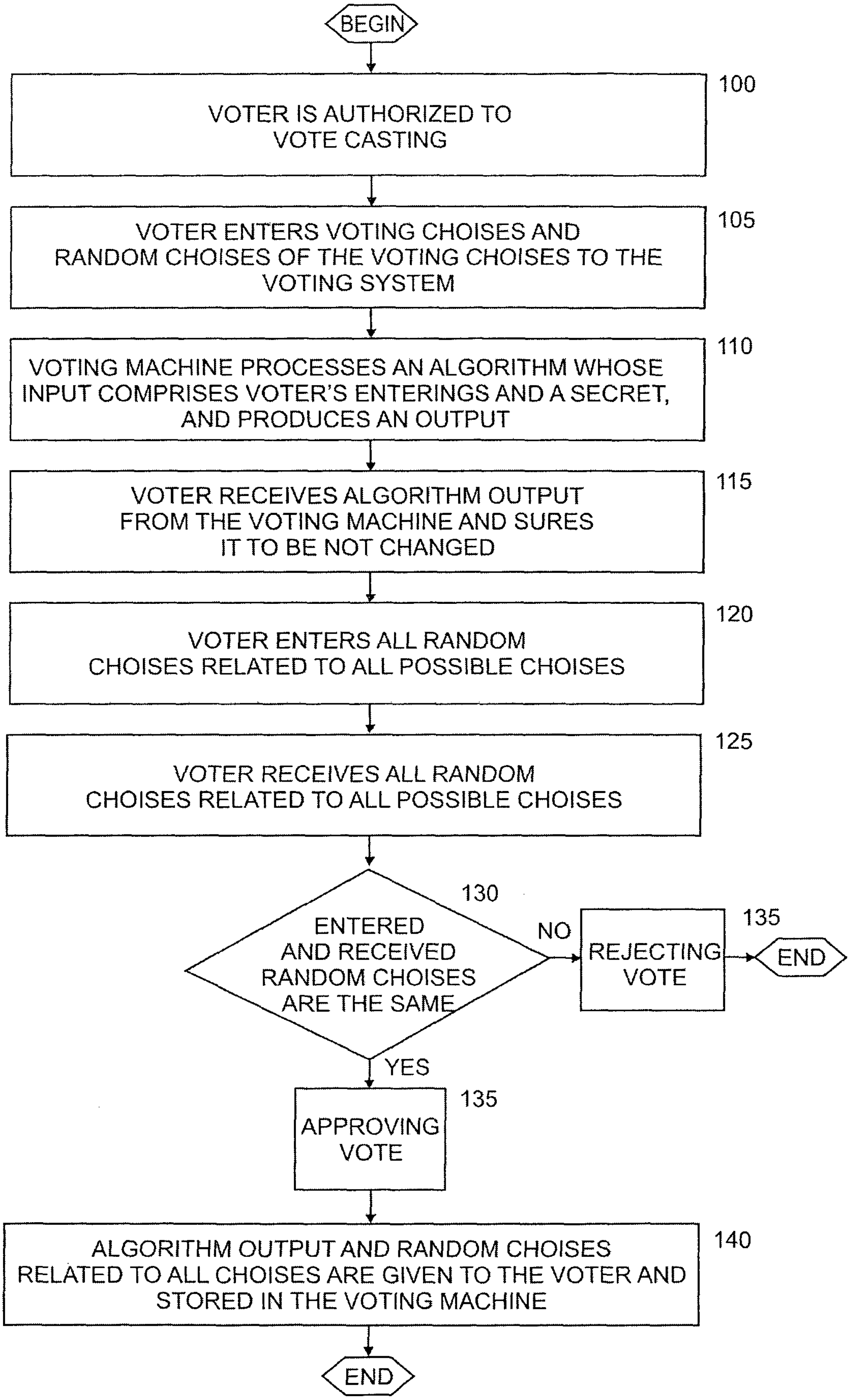
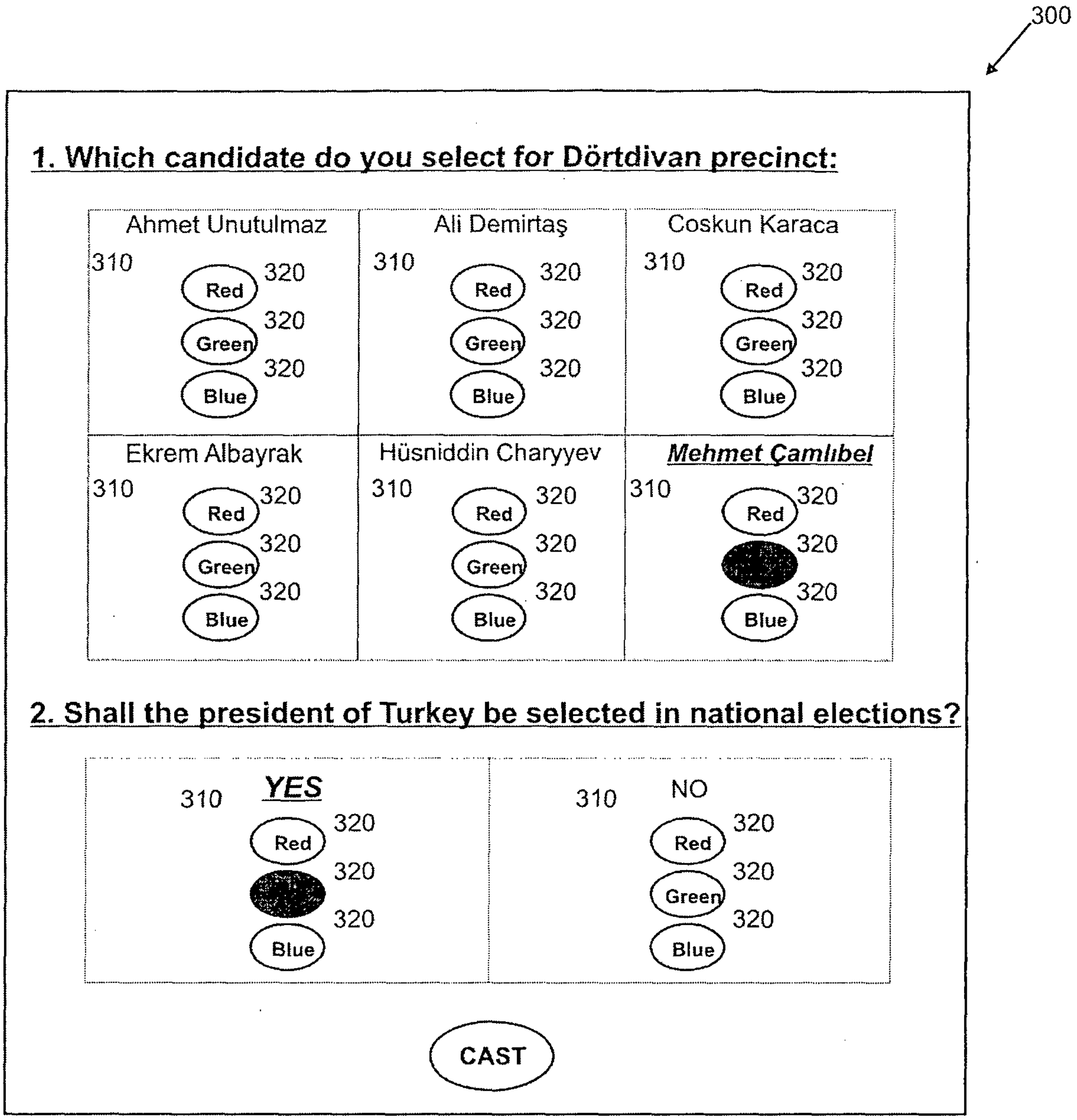

BEGIN
100
VOTER IS AUTHORIZED TO VOTE CASTING
105
VOTER ENTERS VOTING CHOISES AND RANDOM CHOISES OF THE VOTING CHOISES TO THE VOTING SYSTEM
110
VOTING MACHINE PROCESSES AN ALGORITHM WHOSE INPUT COMPRISES VOTER'S ENTERINGS AND A SECRET, AND PRODUCES AN OUTPUT
115
VOTER RECEIVES ALGORITHM OUTPUT FROM THE VOTING MACHINE AND SURES IT TO BE NOT CHANGED
120
VOTER ENTERS ALL RANDOM CHOISES RELATED TO ALL POSSIBLE CHOISES
125
VOTER RECEIVES ALL RANDOM CHOISES RELATED TO ALL POSSIBLE CHOISES
130
ENTERED AND RECEIVED RANDOM CHOISES ARE THE SAME
NO
REJECTING VOTE
135
END
YES
APPROVING VOTE
135
140
ALGORITHM OUTPUT AND RANDOM CHOISES RELATED TO ALL CHOISES ARE GIVEN TO THE VOTER AND STORED IN THE VOTING MACHINE
END

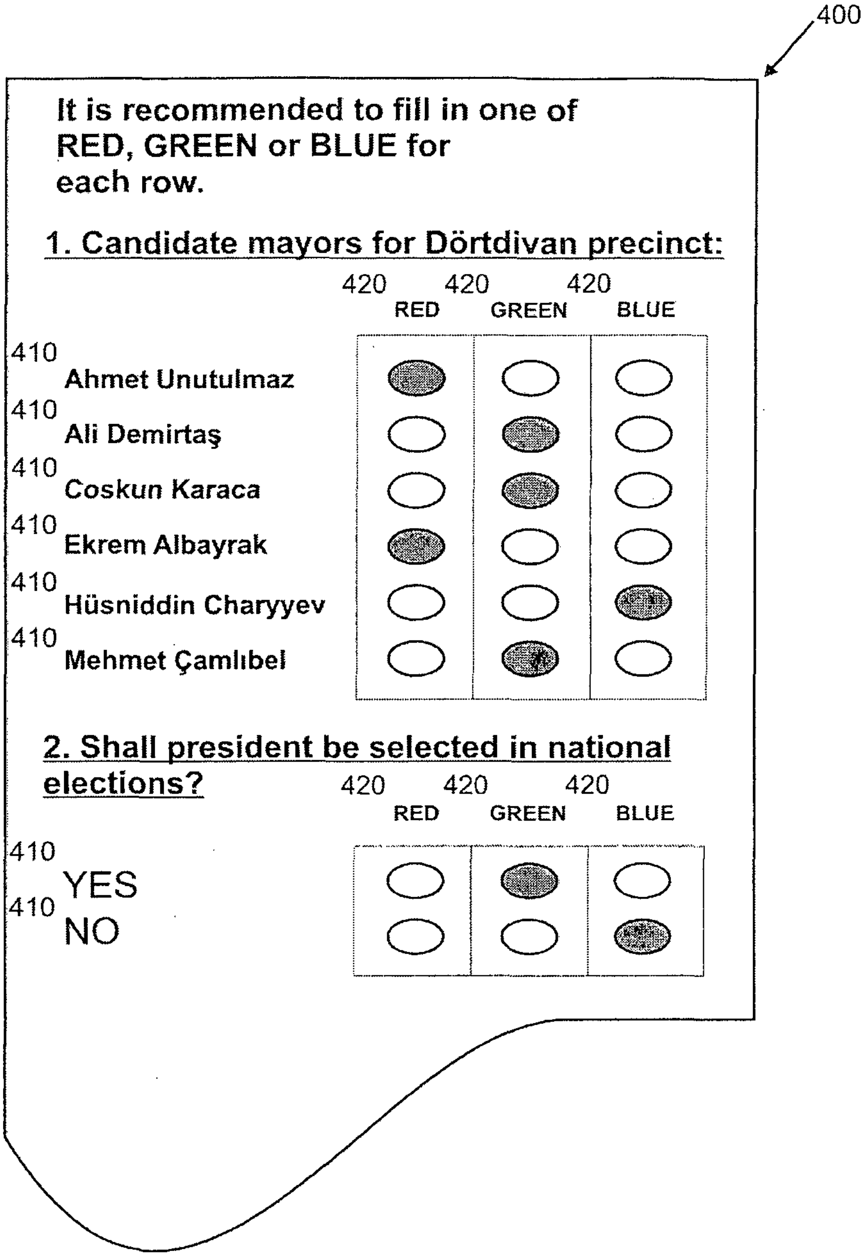
FIGURE 2



1. Which candidate do you select for Dörtdivan precinct:

2. Shall the president of Turkey be selected in national elections?

FIGURE 3



It is recommended to fill in one of RED, GREEN or BLUE for each row.

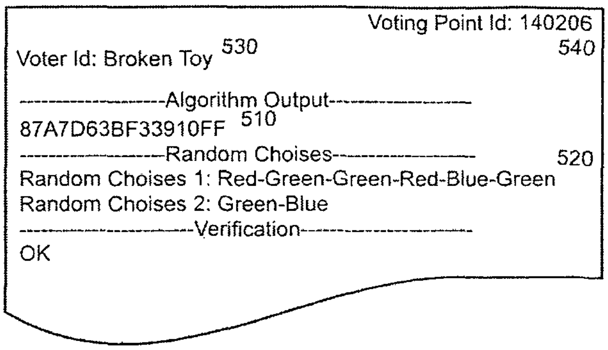
1. Candidate mayors for Dörtdivan precinct:

	RED	GREEN	BLUE
Ahmet Unutulmaz	●	○	○
Ali Demirtaş	○	●	○
Coskun Karaca	○	●	○
Ekrem Albayrak	●	○	○
Hüsniddin Charyyev	○	○	●
Mehmet Çamlıbel	○	●	○

2. Shall president be selected in national elections?

	RED	GREEN	BLUE
YES	○	●	○
NO	○	○	●

FIGURE 4



Voting Point Id: 140206

Voter Id: Broken Toy

------------------Algorithm Output------------------

87A7D63BF33910FF

------------------Random Choises------------------

Random Choises 1: Red-Green-Green-Red-Blue-Green

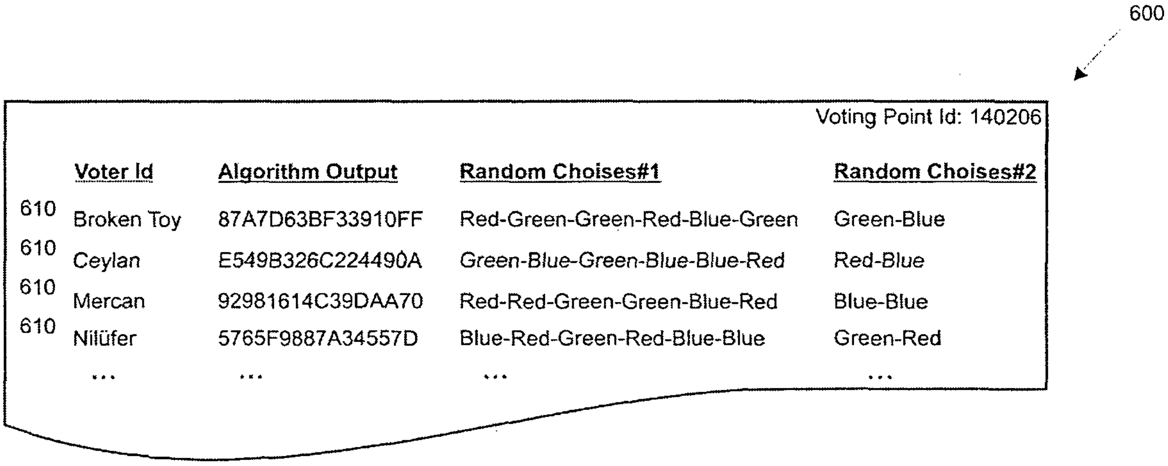
Random Choises 2: Green-Blue

----------------------Verification----------------------

OK

530
540
510
520

FIGURE 5



Voting Point Id: 140206

	Voter Id	Algorithm Output	Random Choises#1	Random Choises#2
610	Broken Toy	87A7D63BF33910FF	Red-Green-Green-Red-Blue-Green	Green-Blue
610	Ceylan	E549B326C224490A	Green-Blue-Green-Blue-Blue-Red	Red-Blue
610	Mercan	92981614C39DAA70	Red-Red-Green-Green-Blue-Red	Blue-Blue
610	Nilüfer	5765F9887A34557D	Blue-Red-Green-Red-Blue-Blue	Green-Red
	...	...	...	...

FIGURE 6

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- US 20080135632 A1 **[0001]**