(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 19/00

(11) 공개번호 특2001-0000030
(43) 공개일자 2001년01월05일

(21) 출원번호 10-1999-0038620
(22) 출원일자 1999년09월10일

(71) 출원인 학교법인 한국정보통신학원 안병엽
서울특별시 종로구 서린동 154-1
(72) 발명자 이병천
대전광역시서구복수동282삼익목화아파트106-2007
김광조
대전광역시서구둔산동삼성한마루아파트7-1406
(74) 대리인 장성구, 이철희

심사청구 : 있음

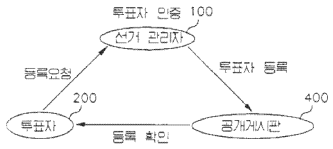
(54) 매수행위 방지 가능한 전자투표 시스템

요약

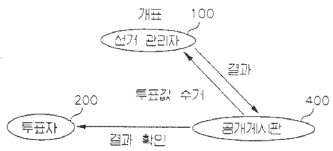
본 발명은 전자투표시스템에 관한 것으로 유권자가 직접 투표소에 출석하여 투표용지에 기표를 하는 통상의 투표방식에서는 막대한 선거관리 비용이 요구된다. 인터넷등 정보통신망의 발전에 따라 암호학적 기법을 이용하여 전자적인 방법으로 선거 시스템을 구현하기 위한 연구가 많이 이루어지고 있다. 비밀분산 및 문턱암호를 이용한 종래의 전자투표 시스템은 매표방지 기능을 제공하지 못하였던 단점이 있었으나 본 발명에서는 비밀정보의 공동생성 기법을 이용하여 매표방지 기능을 제공한다.

대표도

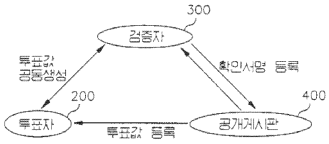
[도 1a]



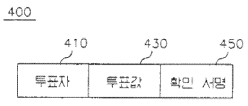
[도 1c]



[도 1b]



[도 1d]



명세서

도면의 간단한 설명

도 1은 본 발명에 따라 여러 단계로 구성되는 전자투표 시스템의 투표과정을 설명하는 구성도,

도 2는 본 발명에 따른 전자투표 시스템에서 수행되는 투표과정의 상세 메시지 계산 및 동작을 설명하는 흐름도.

〈도면의 주요부분에 대한 부호의 설명〉

100 : 선거관리자 200 : 투표자

300 : 검증자 400 : 공개게시판

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 유권자가 투표소에 출석하여 투표용지에 직접 기표하는 통상의 투표 방식을 인터넷 등의 정보통신망을 이용하여 전자적인 방법으로 대체할 수 있도록 하는 암호학적인 기법을 이용한 전자 투표 방법에 관한 것이다.

통상적으로, 물리적인 투표는 투표자와 투표관리자 모두에게 시간적, 공간적, 금전적인 지출을 크게 요구한다. 다시 말해서, 투표자는 투표장소에 직접 출석하여 투표를 해야하기 때문에 시간을 투자해야 하는 불편한 점이 있고, 투표 관리자는 투표소를 설치 및 운용해야 하고 개표작업에도 많은 인력을 필요로 하므로 금전적인 지출이 필요하다. 이러한 통상의 물리적인 투표방식의 불편함을 개선하고자 전자투표 방식이 제안되어 있다.

전자투표는 통상의 물리적인 투표방식을 암호학적 방법을 이용하여 전자적인 방식으로 대체하는 방식으로서, 종래의 물리적인 투표와 비교해볼 때 다음과 같은 특성들을 만족해야 한다.

즉, 투표자의 투표내용을 제 3 자가 알 수 없어야 하는 기밀성과, 모든 유효 투표는 정확하게 계수되어야 하는 완전성과, 부정직한 투표자가 선거를 교란할 수 없어야 하는 건전성과, 투표자는 단 1번만 투표할 수 있어야 하는 이중투표 불가능성과, 투표 권한을 가진 자만이 투표를 할 수 있어야 하는 적임성과, 어떤 것도 선거에 영향을 미쳐서는 안되는 공정성과, 투표내용의 유효성을 검증할 수 있어야 하는 검증성과, 일부의 투표관리 시스템에 문제가 발생하더라도 투표는 계속 진행될 수 있어야 하는 강인성과, 투표권을 매매하는 행위가 불가능해야 하는 매표 방지성이 있어야 한다.

전자투표는 암호학적 프로토콜의 발전과 함께 1980년대에 들어서 연구되기 시작하였으며, 크게 두 가지 부류로 분류될 수 있다. 첫 번째 부류는 은닉서명(blind signature) 기법과 익명통신로(mix-net)를 이용한 방법으로, 1993년 후지오카-오카모토-오타(Fujioka-Okamoto-Ohta)의 연구가 대표적이다. 또 다른 부류는 비밀분산(secret sharing)과 문턱암호(threshold cryptography)를 이용하는 방법으로 1997년 크래머-제나로-쉔마커(Cramer-Gennaro-Schoenmaker)의 연구가 있다.

은닉서명과 익명통신로를 이용하는 후지오카-오카모토-오타(Fujioka- Okamoto-Ohta) 방식은 투표자와 투표값과의 연결을 방지하기 위한 익명통신로가 현실적으로 구현이 어렵고, 투표자와 선거관리자간에 메시지 통신 횟수가 많고, 투표오류 발생시 투표자와 관리자중 누가 부정행위를 했는지 밝혀내기 어렵다는 단점이 있다.

비밀분산과 문턱함호를 이용하는 크래머-제나로-쉔마커(Cramer- Gennaro- Schoenmaker) 방식은 비밀분산으로 인해 시스템의 강인성을 제공하고 문턱암호 기법을 이용하여 개표가 한 번에 이루어질 수 있다는 장점이 있다. 그러나, 크래머-제나로-쉔마커(Cramer-Gennaro-Schoenmaker) 방식은 사용자가 자신의 투표값을 차후 증명할 수 있어서 매표가 가능하다는 단점이 있다. 즉, 투표자는 자신이 투표에 사용했던 난수값을 저장해 놓았다가 매수자에게 제시하면 자신의 투표내용을 증명할 수 있어서 매표에 사용될 수 있다는 문제가 있다.

발명이 이루고자하는 기술적 과제

그러므로, 본 발명은 상술한 문제를 해결하고자 안출된 것으로, 비밀분산과 문턱암호를 이용하는 기법을 바탕으로 매표방지 기능을 제공하는 새로운 전자투표 시스템의 투표 방법을 제공하는 것을 그 목적으로 한다.

본 발명의 다른 목적은 전자투표 시스템을 구현하기 위하여 두 참여자가 정보의 상호 비밀은 유지하면서 비밀정보를 공동으로 생성하는 전자투표 시스템의 투표방법을 제공하는 것이다.

상술한 목적을 달성하기 위한 본 발명에 따른 전자투표 시스템의 투표 방법은, 상기 투표자가 선택한 후보자에 대하여 행한 투표값(x,y)을 상기 검증자에게 전송하는 단계; 상기 검증자가 상기 투표값(x,y)의 증명을 불가능하게 하기 위한 검증자 난수(u,v)를 생성하여 상기 투표자에게 제공하는 단계; 상기 투표자가 상기 투표값(x,y)의 유효성을 증명하고, 그 증명에 대한 응답(d_i,r_i)을 생성하여 상기 검증자에게 제공하는 단계; 상기 응답(d_i,r_i) 에 응답하여, 상기 검증자가 상기 1차 투표값(x,y)의 유효성을 검증하고, 상기 검증자 난수(u,v)의 유효성을 증명하는 응답(r)을 상기 투표자에게 전송하는 단계; 상기 응답(r)에 응답하여, 상기 투표자가 상기 검증자 난수(u,v)의 유효성을 검증하여 유효한 경우 상기 투표값(x,y)과 상기 검증자 난수(u,v)와의 곱셈에 의해 최종 투표값(x_f,y_f)를 계산하여 상기 공개게시판에 게시하는 단계; 상기 검증자가 상기 공개게시판에 게시된 상기 최종 투표값(x_f,y_f)의 유효성을 검증하여 상기 최종 투표값(x_f,y_f)에 대한 확인 서명을 상기 공개게시판에 게시하는 단계를 포함하는 것을 특징으로 한다.

발명의 구성 및 작용

이하 본 발명은 첨부된 도면을 참조하여 다음과 같이 상세히 설명될 것이다.

도 1은 본 발명에 따른 전자투표 시스템의 개략적인 블록 구성도를 도시한 것으로, 전자투표 시스템의 주된 참여자는 선거관리자(100), 투표자(200), 검증자(300), 공개게시판(400)을 포함하며, 이들 각각의 참여자는 컴퓨터 시스템으로 구현될 수 있다. 전자투표 시스템을 구성하는 각각의 참여자는 다음과 같은 기능을 수행한다.

선거관리자(100)는 투표자(200)의 유권자 등록 요청에 따라 신분을 인증한 후 공개게시판(400)에

등록하고 투표후 투표값을 수거하여 개표하는 기능을 수행한다.

투표자(200)는 선거관리자(100)에게 유권자 등록을 요청하여 공개게시판(400)에 유효한 투표자로 등록받은 후 검증자(300)와의 상호작용을 통하여 자신의 최초 투표값과 검증자(300)가 제공하는 검증자 난수를 곱하여 최종 투표값을 계산하고 이를 공개게시판(400)에 등록하는 역할을 담당한다.

검증자(300)는 투표자(200)의 투표의 유효성을 검증하고 검증자 난수를 발생하여 투표자(200)에게 제공하고 최종 투표값이 유효한지를 검증하여 공개게시판(400)에 확인 서명을 등록하는 기능을 수행한다.

공개게시판(400)은 투표자(200)를 등록하고 투표자(200)의 투표값을 게시하며, 검증자(300)의 확인서명을 게시하는 공개게시판 역할을 담당한다. 공개게시판(400)은 투표자(200)의 이름이 게시되는 이름란(410), 투표자(200)의 최종 투표값이 게시되는 투표란(430) 및 검증자(300)에 의해 최종 투표값에 대한 확인서명이 게시되는 서명란(450)을 구비한다. 공개게시판(400)에 게시된 모든 내용은 각 투표자(200) 및 검증자(300)에 의해 검색될 수 있지만, 각 투표자(200) 및 검증자(300)는 공개게시판(400)에서 자신에게 할당된 영역에만 메시지를 게시할 수 있다.

상술한 참여자로 구성되는 본 발명의 전자투표 시스템은 순서적으로 도 1a의 투표자 등록과정, 도 1b의 투표과정 및 도 1c의 개표과정을 통하여 동작하는 것으로, 본 발명은 투표자(200)와 검증자(300)가 최종 투표값을 공동으로 생성하는 투표과정의 프로토콜에 관련된다.

도 1a의 투표자 등록과정에서, 투표자(200)는 유권자로서 등록을 위하여 자신의 신분을 확인할 수 있는 개인정보를 포함하는 등록요청 메시지를 선거관리자(100)에게 전송한다. 선거관리자(100)는 투표자(200)의 등록요청 메시지에 응답하여 투표자(200)의 신분을 확인한 후 공개게시판(400)에 유효한 투표자(200)로 등록한다. 투표자(200)는 자신의 등록여부를 공개게시판(400)으로부터 확인할 수 있다.

도 1b의 투표과정에서, 투표자(200)와 검증자(300)는 하기 설명되는 투표 프로토콜을 이용하여 투표자(200)가 생성하는 1차 투표값과 검증자(300)가 생성하는 검증자 난수를 곱하여 최종 투표값을 공동으로 생성한다. 투표자(200)는 생성된 최종 투표값을 공개게시판(400)에 등록하고 검증자(300)는 최종 투표값의 유효성을 검증한 후 공개게시판(400)에 확인 서명을 등록한다.

도 1c의 개표과정에서, 선거관리자(100)는 투표가 종료된 후 공개게시판(400)에 등록된 모든 투표값들을 수거하고 자신의 개인키를 이용하여 개표하여 투표결과를 계산하고 이를 다시 공개게시판(400)에 등록한다. 투표자(200)는 투표결과를 공개게시판(400)으로부터 확인할 수 있다.

본 발명의 전자투표 시스템은 투표값을 계산하기 위하여 이산대수 문제에 기반한 엘가말(Elgamal)형의 공개키 암호 시스템을 사용한다. 선거관리자(100)는 엘가말형의 개인 키와 공개키 쌍을 생성하여 개인키는 비밀히 보관하고 공개키는 인증기관으로부터 공개키 인증서의 형태로 발급받고 이를 공개게시판(400)에 게시하여 모든 투표자(200)가 이용할 수 있도록 한다. 복수의 선거관리자(100)를 이용할 경우에는 잘 알려진 비밀분산 기법을 이용하여 공개키를 공동으로 생성하고 비밀키를 분산시켜서 투표의 기밀성을 보다 완벽히 보호할 수 있고 전자투표 시스템의 강인성을 제공할 수도 있다. 각 투표자(200) 및 검증자(300)는 마찬가지로 인증기관으로부터 공개키 인증서를 발급받아서 상호 인증에 사용한다.

본 발명의 주요 특징인 도 1b에 예시된 투표단계의 메시지 흐름은 도 2의 흐름도를 참조하여 보다 상세히 설명된다.

단계(510)에서, 투표자(200)는 k명의 입후보자(G) 중 한명, 예를 들면 i 번째 후보자(G_i) (여기서, $1 \le i \le k$)를 선택한 다음, 임의의 난수(α)(여기서, $\alpha \in_R Z_q$ 를 만족하는 난수)를 선정하여 i 번째 후보자에 대한 투표로서 하기 수학식 1과 같은 1차 투표값(x,y)을 계산한다.

$$(x,y) = (g^{a}, h^{a}G_{i})$$

상술한 수학식 1에서, g는 갈로아 필드 "GF(p)"의 생성자(generator)이고, p는 갈로아 필드(GF(p))를 생성하는 소수이고, h는 선거관리자(100)의 공개키((h = g^{s} mod p))이고, G_i는 k명의 후보자를 나타내는 서로 독립적인 생성자를 의미한다.

그 다음 단계(520)에서, 투표자(200)는 임의의 난수(w_1)(여기서, $w_1 \in_R Z_q$ 를 만족하는 난수)를 선택하여 하기 수학식 2와 같이 1차 투표값(x,y)의 암호화를 위한 난수값(a_i,b_i)을 계산하며, i가 아닌 나머지 k-1개의 j에 대하여(j=1, . . . , i-1, i+1, . . . , k) 임의의 난수값(d_j, r_j)(여기서, $d_j, r_j \in_R Z_q$를 만족함)를 선정한 후 하기 수학식 3에 의해 1차 투표값(x,y)을 암호화하여 암호화된 1차 투표값(a_j, b_j)(=(a_1, b_1),....(a_k, b_k))을 계산한다. 이렇게 계산된 암호화된 1차 투표값들(a_j, b_j)은 1차 투표값(x,y)의 유효성을 증명하는 데 사용된다. 이후 암호화된 1차 투표값들(a_j, b_j)은 간단히 난수값 (A, B)로 정의한다.

$$(a_i, b_i)=(g^{w1}, h^{w1})$$

$$(a_j, b_j)=(g^{rj}x^{dj}, h^{rj}(y/G_j)^{dj})$$

그 다음 단계(530)에서, 투표자(200)는 1차 투표값(x,y)과 암호화된 1차 투표값(A, B)을 검증자(300)에게 전송한다.

단계(540)에서, 검증자(300)는 임의의 난수 β와 w_2(여기서, $\beta, w_2 \in_R Z_q$ 를 만족하는 난수)를 선정하여 하기 수학식 4 및 5를 이용하여 검증자 난수(u,v) 및 (a, b)를 계산한다. 검증자 난수(u,v)는 검증자(300)가 생성하여 투표자(200)에게 제공하는 난수로서 투표의 증명을 불가능하게 하는데 사용된다.

$$(u,v)=(g^{\beta},h^{\beta})$$

$$(a,b)=(g^{w2},h^{w2})$$

이와 함께 검증자(300)는 1차 투표값(x,y)의 유효성 증명을 위한 시도로서 임의의 난수(c_1)(여기서, $c_1 \in_R Z_q$을 만족하는 난수)를 선택한 다음, 검증자 난수(u,v)와 (a,b) 및 임의의 난수(c_1)를 투표자(200)에게 전송한다(단계 550).

그 다음 단계(560)에서, 투표자(200)는 검증자의 유효성 증명을 위한 임의의 난수(c_1)를 이용하여 1차 투표값의 유효성을 증명한 응답(d_i, r_k)을 하기 수학식 6과 같이 계산한다.

$$(d_i, r_i)=(c_1-\sum d_j, w_1 - ad_i)$$

이때 k개의 (d_i, r_i), 즉 (d_1, r_1),...(d_k, r_k)를 (D, R) 이라 하면, 이것은 1차 투표값의 유효성에 대한 응답이 된다.

또한, 투표자(200)는 검증자(300)로부터 제공된 검증자 난수(u,v)의 유효성을 증명하기 위한 시도로서 임의의 난수(c_2)(여기서, $c_2 \in_R Z_q$을 만족하는 난수)를 선택하고, 1차 투표의 유효성에 대한 응답값(D, R)과 임의의 난수(c_2)를 검증자(300)에게 송신한다(단계 570).

그 다음 단계(580)에서, 검증자(300)는 1차 투표값(x,y)의 유효성을 검증하기 위하여 (D, R), (A, B), 임의의 난수(c_1)를 이용하여 하기 수학식 7 및 8과 같은 제시된 조건을 만족하는지를 검사한다.

$$c_1 = d_1 + ..., + d_k$$

for $j=1,...k$

$$(a_j, d_j) = (g^{rj} x^{dj}, h^{rj}(y/G_j)^{dj})$$

또한, 검증자(300)는 검증자 난수(u, v)의 유효성을 증명하기 위하여 투표자로부터 제공된 임의의 난수(c_2)에 대한 응답(r)을 하기 수학식 9와 같이 계산한 다음, 투표자(200)에게 계산된 응답(r)을 전송한다.

$$r = w_2 + \beta c_2$$

그 다음 단계(590)에서, 투표자(200)는 검증자(300)로부터 제공된 검증자 난수(u,v)의 유효성을 검증하기 위하여 하기 수학식 10을 이용하여 검증자 난수의 유효성 증명(g^r, h^r)을 계산한다.

$$(g^r, h^r) = (au^{c1}, bv^{c1})$$

상술한 수학식 10으로부터 검증자 난수(u,v)의 유효성이 유효한 것으로 검증되면, 1차 투표값(x,y)과 검증자 난수(u,v)를 곱해서 최종 투표값(x_f, y_f)(=(xu, yv))을 계산하고 계산된 최종 투표값(x_f, y_f)을 공개게시판(400)의 투표란(430)에 게시한다. 이와 같이, 최종 투표값(x_f, y_f)을 투표자(200)와 검증자(300)가 공동으로 생성함으로써, 투표자(200)는 제 3의 매수자에게 자신의 투표 내용을 증명할 수 없어서 매표를 방지할 수 있다.

이후, 단계(600)에서, 검증자(300)는 공개게시판(400)의 투표란(430))에 게시된 투표자(200)의 최종 투표값(x_f, y_f)의 유효성을 하기 수학식 11과 같이 검증하고 투표가 유효한 경우 하기 수학식 12와 같은 확인 서명을 서명란(450)에 게시한다.

$$(x_f, y_f) = (xu, yv)$$

$$Sig(H(ID, x_f, y_f, Time, OK))$$

이후, 도 2를 참조하여 설명된 투표 과정이 종료된 후, 도 1c에 예시된 개표과정에서는 선거관리자(100)가 공개게시판(400)에 게시된 모든 유효한 최종 투표값들을 모아서 이들의 최종 곱을 계산한 후 선거관리자(100)의 개인키를 이용하여 복호화함으로써 최종 결과를 얻을 수 있다.

상술한 본 발명의 투표자와 검증자와의 상호작용에 의해 투표값을 공동으로 생성하는 방식은 전자투표 뿐만 아니라, 두 참여자가 상호 비밀을 유지하면서 비밀정보를 공동으로 생성하는 것을 필요로 하는 여타의 다른 응용분야에도 적용될 수 있다. 예를 들면, 제 1 참여자의 비밀정보를 여타 참여자에게 증명할 수 없도록 하고자 할 때, 제 2 참여자는 제 1 참여자의 비밀정보를 알 수 없도록 하는 대신, 비밀정보의 유효성은 검증할 수 있도록 하고, 제 1 참여자는 제 2 참여자가 제공하는 난수정보의 비밀을 알 수 없도록 하는 대신, 이의 유효성은 검증할 수 있도록 하며, 최종 비밀번호는 제 1 참여자의 비밀정보와 제 2 참여자의 난수정보를 곱하여 생성하도록 함으로써, 두 참여자에 의해 공동 생성된 비밀정보를 비밀히 보존할 수 있다.

발명의 효과

그러므로, 본 발명에 따른 전자투표 시스템에서 최종 투표값을 계산함에 있어서, 투표자가 생성한 1차 투표값과 검증자가 제공한 검증자 난수를 곱하여 계산함으로, 최종 투표값을 투표자와 검증자가 공동으로 생성하게 된다. 그러므로, 투표자는 제 3 의 매수자에게 자신의 투표 내용을 증명할 수 없어서 매표방지 기능이 제공될 수 있다. 또한, 본 발명의 전자투표 시스템에서 수행되는 방법을 통하여 검증자는 투표내용의 유효성을 검증할 수는 있으나, 구체적인 투표내용은 알 수 없기 때문에 검증성과 기밀성이 보장될 수 있다. 본 발명은 종래기술의 비밀분산, 문턱암호를 이용하는 전자투표 시스템에서 매표방지 기능을 추가적으로 제공할 수 있다.

(57) 청구의 범위

청구항 1

비밀 내용을 제 3의 매수자에게 증명할 수 없도록 하는 비밀정보 암호화 방법에 있어서,

상기 제 1 참여자가 상기 비밀내용을 포함하는 비밀정보를 생성하여 상기 제 2 참여자에게 제공하는 단계;

상기 제 2 참여자가 상기 비밀정보의 증명을 불가능하게 하는 난수정보를 생성하여 상기 제 1 참여자에게 제공하는 단계;

상기 제 1 참여자가 상기 비밀정보의 유효성을 증명하고, 상기 비밀정보의 유효성 증명을 상기 제 2 참여자에게 제공하는 단계;

상기 제 2 참여자가 상기 비밀정보의 유효성을 검증하고, 상기 난수정보의 유효성을 증명하여, 상기 난수정보의 유효성 증명을 상기 제 1 참여자에게 제공하는 단계;

상기 제 1 참여자가 상기 난수정보의 유효성을 검증하고, 상기 검증된 난수정보와 상기 비밀정보를 곱셈하여 최종 비밀정보를 생성하는 것을 특징으로 하는 비밀정보의 암호화 방법.

청구항 2

투표자, 검증자 및 공개게시판으로 구성된 전자투표 시스템의 투표 방법에 있어서,

상기 투표자가 선택한 후보자에 대하여 행한 투표값(x,y)을 상기 검증자에게 전송하는 단계;

상기 검증자가 상기 투표자가 행한 투표값(x,y)의 증명을 불가능하게 하기위한 검증자 난수(u,v)를 생성하여 상기 투표자에게 제공하는 단계;

상기 투표자가 상기 투표값(x,y)의 유효성을 증명하고, 그 증명에 대한 응답(d_i, r_i)을 생성하여 상기 검증자에게 제공하는 단계;

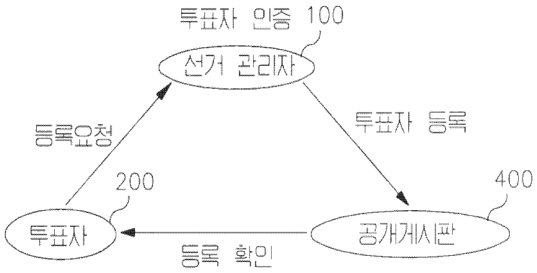
상기 응답(d_i, r_i)에 응답하여, 검증자가 상기 투표값(x, y)의 유효성을 검증하고, 상기 검증자 난수(u, v)의 유효성을 증명하는 응답(r)을 상기 투표자에게 전송하는 단계;

상기 응답(r)에 응답하여, 상기 투표자가 상기 검증자 난수(u,v)의 유효성을 검증하여 상기 1차 투표값(x,y)과 상기 검증자 난수(u,v)와의 곱셈에 의해 최종 투표값(x_f, y_f)를 계산하여 상기 공개게시판에 게시하는 단계;

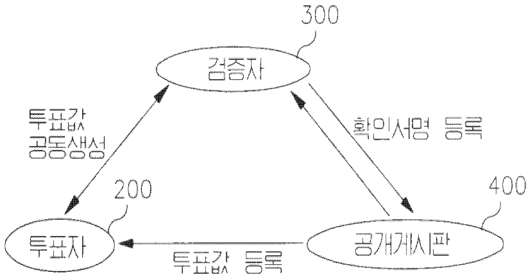
상기 검증자가 상기 공개게시판에 게시된 상기 최종 투표값(x_f, y_f)의 유효성을 검증하여 상기 최종 투표값(x_f, y_f)에 대한 확인 서명을 상기 공개게시판에 게시하는 단계를 포함하는 것을 특징으로 하는 전자 투표시스템의 투표방법.

도면

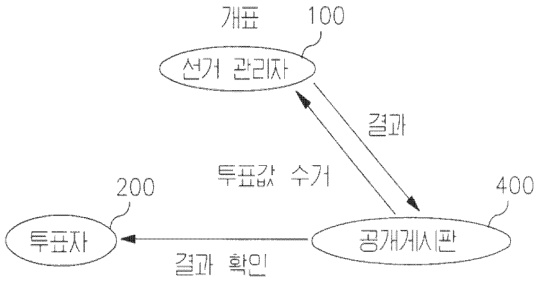
도면1a



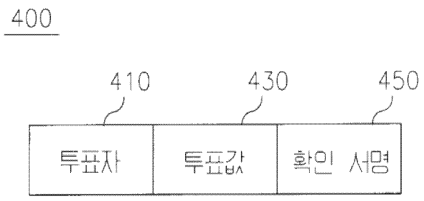
도면1b



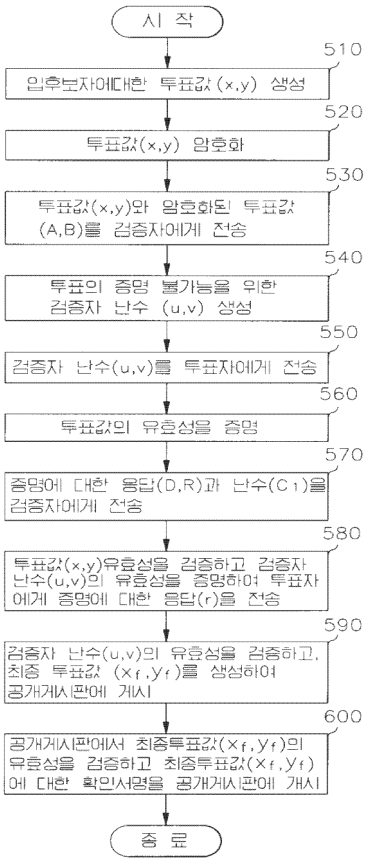
도면1c



도면1d



도면2


시 작
510
입후보자에대한 투표값(x,y) 생성
520
투표값(x,y) 암호화
530
투표값(x,y)와 암호화된 투표값 (A,B)를 검증자에게 전송
540
투표의 증명 불가능을 위한 검증자 난수 (u,v) 생성
550
검증자 난수(u,v)를 투표자에게 전송
560
투표값의 유효성을 증명
570
증명에 대한 응답(D,R)과 난수(C1)을 검증자에게 전송
580
투표값(x,y)유효성을 검증하고 검증자 난수(u,v)의 유효성을 증명하여 투표자에게 증명에 대한 응답(r)을 전송
590
검증자 난수(u,v)의 유효성을 검증하고, 최종 투표값 (xf,yf)를 생성하여 공개게시판에 게시
600
공개게시판에서 최종투표값(xf,yf)의 유효성을 검증하고 최종투표값(xf,yf)에 대한 확인서명을 공개게시판에 게시
종 료