(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년08월18일
(11) 등록번호 10-0912532
(24) 등록일자 2009년08월10일

(51) Int. Cl.
G06Q 50/00 (2006.01)
(21) 출원번호 10-2007-0038314
(22) 출원일자 2007년04월19일
심사청구일자 2007년04월19일
(65) 공개번호 10-2009-0001497
(43) 공개일자 2009년01월09일
(30) 우선권주장
1020060120453 2006년12월01일 대한민국(KR)
(56) 선행기술조사문헌
KR1020050116050 A*
US20060020781 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
김영수
대전 유성구 반석동 양지마을2단지 209동1106호
전성익
대전 유성구 어은동 한빛아파트 107동 704호
(74) 대리인
특허법인 씨엔에스 · 로고스

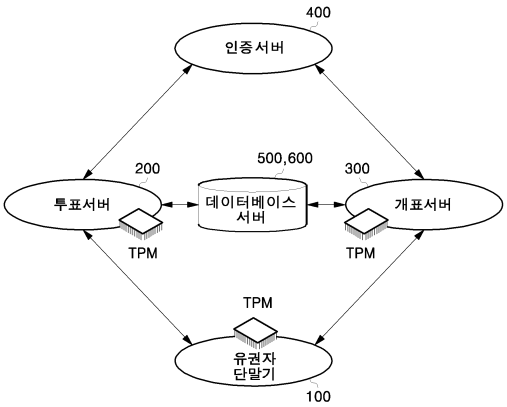
전체 청구항 수 : 총 10 항 심사관 : 전한철

(54) 신뢰 컴퓨팅 환경에서 각 참여자가 상호 보증 기능을 갖는인터넷 전자투표 방법 및 시스템

(57) 요 약

본 발명은 신뢰 컴퓨팅 환경에서 각 참여자가 상호 보증 기능을 갖는 인터넷 전자투표 방법 및 시스템에 관한 것으로, 상기 유권자 단말기, 투표서버, 및 개표서버 각각은 TPM을 이용하여 상기 인증서버로부터 자신의 인증서를 제공받고, 상기 투표서버와 개표서버는 자신의 인증서를 서로 교환한 후 투표 처리 정보와 개표 처리 정보를 각각 생성하는 전처리 과정; 상기 유권자 단말기, 상기 투표서버 및 상기 개표서버가 상기 TPM을 이용하여 서로를 보증한 후, 상기 개표서버가 상기 유권자 단말기에서 생성된 투표횟수를 통해 이중 투표를 검사하고, 상기 유권자 단말기가 투표 정보를 생성하면, 상기 투표서버가 상기 투표 처리 정보에 따라 상기 투표 정보를 저장하는 투표 과정; 및 상기 저장된 투표 정보를 상기 개표 처리 정보에 따라 분석하여 투표 내용을 집계하고 출력하는 개표 과정을 포함하여 구성되며, 이에 의하여 유권자 단말기, 투표서버 및 개표서버는 TPM을 이용하여 자신의 성능을 극대화하는 동시에 유권자 단말기와 서버들이 스스로 보증 주체가 될 수 있도록 하여, 투표의 신뢰성을 증대시켜 준다.

대 표 도 - 도1



특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

유권자 단말기, 투표서버, 개표서버 및 인증서버를 참여자로 가지는 인터넷 전자투표 방법에 있어서,

상기 유권자 단말기, 투표서버 및 개표서버 각각은 TPM(Trusted Platform Module)을 이용하여 상기 인증서버로부터 자신의 인증서를 제공받고, 상기 투표서버와 상기 개표서버는 자신의 인증서를 서로 교환한 후 투표 처리 정보와 개표 처리 정보를 각각 생성하는 전처리 과정;

상기 유권자 단말기, 상기 투표서버 및 상기 개표서버가 상기 TPM을 이용하여 서로를 보증한 후, 상기 개표서버가 상기 유권자 단말기에서 생성된 투표횟수를 통해 이중 투표를 검사하고, 상기 유권자 단말기가 투표 정보를 생성하면, 상기 투표서버는 상기 투표 처리 정보에 따라 상기 투표 정보를 저장하는 투표 과정; 및

상기 저장된 투표 정보를 상기 개표 처리 정보에 따라 분석하여 투표 내용을 집계하고 출력하는 개표 과정을 포함하되,

상기 투표 과정은

상기 유권자 단말기가 제1 난수, 상기 투표횟수, 투표횟수의 제1 해쉬값, 및 투표시간, 그리고 유권자 TPM 정보를 생성하여 상기 투표서버와 상기 개표서버로 전송하는 제1 단계;

상기 투표서버와 상기 개표서버 각각이 상기 유권자 TPM 정보를 통해 상기 유권자 단말기의 보증을 확인하고 상기 투표횟수를 통해 이중 투표를 검사한 후, 투표서버 TPM 정보와 개표서버 TPM 정보를 생성하여 상기 유권자 단말기로 전송하는 제2 단계;

상기 유권자 단말기가 상기 투표서버 TPM 정보와 상기 개표서버 TPM 정보를 이용하여 상기 투표서버와 상기 개표서버 각각의 신뢰성을 확인하는 제3 단계;

상기 개표서버가 제2 난수를 더 생성한 후, 상기 개표서버와 상기 유권자 단말기가 상기 제2 난수와 상기 제1 난수를 이용하여 세션키를 생성하는 제4 단계;

상기 개표서버가 상기 개표 처리 정보에 포함된 투표 티켓들 중 하나를 선택하여 상기 유권자 단말기에게 제공하고, 상기 유권자 단말기는 상기 투표 티켓을 획득하여 투표값 및 서명된 투표값을 포함하는 상기 투표 정보를 생성한 후 상기 투표서버에게 전송하는 제5 단계;

상기 투표서버가 상기 서명된 투표값을 검증한 후 상기 유권자 단말기의 정보를 저장하고, 상기 유권자 단말기는 상기 투표횟수를 상기 개표서버로 전송하는 제6 단계; 및

상기 개표서버가 상기 투표횟수를 통해 투표가 정상 수행되었음을 확인하면, 상기 투표서버는 상기 무작위 수열에 상기 투표값 및 상기 서명된 투표값를 매핑하여 저장하는 제7 단계를 구비하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 4

제3항에 있어서, 상기 유권자 TPM 정보는

하기의 수학식과 같은 유권자 서명값, 유권자 인증서, 유권자 검증키, 및 플랫폼의 측정값 리스트를 포함하는 것을 특징으로 하는 인터넷 전자투표 방법.

$$S=SIG_{AIK\_Vi\_비밀키}(H(RN) \| TS \| PCR)$$

여기서, S는 상기 유권자 서명값, AIK_Vi_비밀키는 상기 유권자 서명키, RN는 상기 투표횟수, H(RN)는 상기 투

표횟수의 제1 해쉬값, TS는 상기 투표시간, PCR는 플랫폼의 측정값, $SIG_X(Y)$는 X키로 하는 Y에 대한 서명 함수이다.

청구항 5

제4항에 있어서, 상기 제2 단계는

상기 투표서버 및 상기 개표서버 각각이 상기 유권자 인증서를 이용하여 상기 유권자 검증키를 확인하고, 상기 유권자 서명값을 검증하여 상기 플랫폼의 측정값을 획득한 후, 상기 플랫폼의 측정값 리스트와 비교함으로써 상기 유권자 단말기의 보증을 확인하는 단계; 및

상기 유권자 단말기의 보증을 확인한 상기 투표서버와 상기 개표서버 각각이 상기 투표횟수의 저장여부를 조사하여 이중 투표 여부를 확인한 후, 상기 투표서버 TPM 정보와 상기 개표서버 TPM 정보를 각각 생성하여 상기 유권자 단말기에 전송하는 단계를 구비하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 6

제4항에 있어서,

상기 투표서버 TPM 정보는 상기 투표서버 인증서, 상기 투표서버 검증키, 상기 투표서버 서명값, 및 상기 플랫폼의 측정값 리스트를 포함하고,

상기 개표서버 TPM 정보는 상기 개표서버 인증서, 상기 개표서버 검증키, 상기 개표서버 서명값, 및 상기 플랫폼의 측정값 리스트를 포함하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 7

제6항에 있어서, 상기 제3 단계는

상기 유권자 단말기가 상기 투표서버 인증서를 이용하여 상기 투표서버 검증키를 확인하고, 상기 투표서버 검증키를 이용하여 상기 투표서버 서명값을 검증하여 상기 플랫폼의 측정값을 획득한 후, 상기 플랫폼의 측정값 리스트와 비교함으로써 상기 투표서버의 보증을 확인하는 단계; 및

상기 유권자 단말기가 상기 개표서버 인증서를 이용하여 상기 개표서버 공개키를 확인하고, 상기 개표서버 공개키를 이용하여 상기 개표서버 서명값을 검증하여 상기 플랫폼의 측정값을 획득한 후, 상기 플랫폼의 측정값 리스트와 비교함으로써 상기 개표서버의 보증을 확인하는 단계를 구비하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 8

제6항에 있어서, 상기 제4 단계는

상기 개표서버가 상기 제2 난수를 더 생성하고, 상기 유권자 서명키로 암호화하여 상기 유권자 단말기로 전송하는 단계;

상기 유권자 단말기가 상기 개표서버로부터 전송되는 암호화된 제2 난수를 복호화한 후, 다시 상기 제1 난수로 암호화하여 상기 개표서버에 전송하는 단계; 및

상기 유권자 단말기가 상기 제2 난수와 상기 제1 난수를 이용하여 상기 세션키를 생성하는 단계를 구비하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 9

제8항에 있어서, 상기 제5 단계는

상기 개표서버가 상기 유권자 단말기로부터 전송되는 암호화된 제2 난수를 복호화하여 상기 제1 난수와 상기 세션키를 획득하고, 상기 투표 티켓들 중 하나를 선택한 후 상기 세션키로 암호화하여 상기 유권자 단말기로 전송하는 단계; 및

상기 유권자 단말기가 상기 암호화된 투표 티켓을 복호화한 후 상기 투표값을 생성하고, 상기 투표값을 상기 유권자 서명키로 서명하여 상기 서명된 투표값을 생성한 후, 상기 투표값과 상기 서명된 투표값을 상기 투표서버

에게 전송하는 단계를 구비하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 10

제9항에 있어서, 상기 제6 단계는

상기 투표서버가 상기 서명된 투표값을 검증하여, 투표와 관련된 상기 유권자 단말기의 정보를 모두 저장하고, 상기 투표값을 상기 투표서버 비밀키로 서명하여 상기 유권자 단말기로 전송하는 단계; 및

상기 유권자 단말기가 상기 투표서버가 제공하는 서명된 투표값을 검증한 후, 상기 투표횟수를 상기 세션키로 암호화하여 상기 개표서버로 전송하는 단계를 구비하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 11

제10항에 있어서, 상기 제7 단계는

상기 개표서버가 상기 유권자 단말기가 제공하는 암호화된 투표횟수를 분석하여, 올바른 투표횟수가 전송되었는지 상기 투표서버가 올바른 정보를 저장하였는지를 검사하고, 상기 검사가 성공하면 상기 투표횟수의 제2 해쉬값을 생성하여 상기 유권자 단말기에 전송한 후 상기 투표횟수를 저장하는 단계;

상기 유권자 단말기는 상기 개표서버가 상기 투표횟수의 제2 해쉬값으로부터 상기 투표 횟수를 획득하여, 투표의 정상 수행 여부를 확인한 후 상기 투표횟수의 제3 해쉬값을 생성하여 상기 투표서버에 전송하는 단계; 및

상기 투표서버는 상기 투표횟수의 제3 해쉬값으로부터 상기 투표 횟수를 획득하여, 투표의 정상 수행 여부를 확인한 후 상기 투표값 및 상기 서명된 투표값에 상기 무작위 수열을 매핑하여 저장하는 단계를 구비하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 12

제3항에 있어서, 상기 개표 과정은

상기 투표서버가 투표값과 서명된 투표값을 포함하는 상기 투표 정보를 자신의 무작위 수열에 따라 정렬한 후, 상기 개표서버에 제공하는 단계;

상기 개표서버가 상기 투표서버가 제공한 상기 투표값과 상기 서명된 투표값을 자신의 무작위 수열에 따라 정렬한 후, 공개 및 개표하는 단계;

상기 개표서버가 투표 마감자수와 투표수가 일치하는지를 검사한 후, 투표서버 검증키로 상기 서명된 투표값의 서명을 검증하고, 개표서버 서명키로 복호화하여 투표내용, 투표 티켓, 및 비밀 번호를 추출하는 단계; 및

상기 개표서버가 상기 투표 티켓을 참조하여 올바른 투표 티켓이 포함되었는지 및 개수가 일치하는지를 검사한 후, 상기 투표내용을 집계하여 발표하는 단계를 구비하는 것을 특징으로 하는 인터넷 전자투표 방법.

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<7> 본 발명은 인터넷 전자투표 방법 및 시스템에 관한 것으로, 특히 TPM(Trusted Platform Module) 기술을 이용하여 각 참여자가 상호 보증 기능을 갖는 인터넷 전자투표 방법 및 시스템에 관한 것이다.

<8> 일반적으로, 전자투표(electronic voting)는 전자적 수단에 의한 투표행위나 투표집계 등 투표의 모든 측면에 응용된 개념을 말한다. 즉, 전자투표 실시를 위해 한 부분 또는 다양한 부분에서 전자적 수단의 조합이 가능하다. 실제 전자적 수단에 의한 투표집계는 이미 세계적으로 상당부분 도입되어 있으며 그 효과가 입증되었다.

<9> 전자투표는 크게 지정된 장소에서 전자기기를 이용하는 방식과 원격투표방식 즉, 지정된 장소가 아닌 다양한 장소에서 투표하는 방식으로 나눌 수 있다.

<10> 먼저, 지정된 장소에서 전자기기를 이용하는 방식은 투표소, 관공서, 쇼핑센터 등 사람들이 자주 모이거나, 접근이 용이한 장소에 전자기기를 설치하고 투표하는 방식을 말하며, 터치스크린 시스템, PC 기반 기술, 그리고 고정식/이동식 키오스크(kiosks) 방식으로 구분된다.

<11> 이중, 키오스크 방식은 투표의 편의증진을 위해 투표소가 아닌 선거구내의 편리한 공공기관이나 장소에 설치된 무인자동안내시스템과 유사한 투표전용기기를 이용한 전자투표방식으로, 다양한 장소로 이동이 가능하며 키패드나 터치스크린 기술을 활용한다.

<12> 상기 방식은 기존의 방식과 같이 투표소에 나와 투표를 해야 하는 점이 불편하지만, 편리하고 쉬운 사용자 인터페이스를 제공하고, 개표 및 집계과정이 신속하며, 무효표 발생 확률이 거의 없다는 점이 장점이다. 무엇보다, 보안상의 위험이 인터넷투표보다 낮다는 차원에서 유력한 차세대 전자투표 방식으로 꼽힌다.

<13> 원격투표방식은 지정된 투표장소가 아닌 다양한 장소에서 다른 여러 전자적 기술을 활용하여 투표하는 것을 의미하며, 전화 투표 방식, 단문 서비스 텍스트 투표방식, 양방향 디지털 TV를 이용한 투표 방식, 그리고 인터넷 투표 방식 등이 있다.

<14> 이중 인터넷 투표 방식은 인터넷을 이용하여 시민들이 어느 장소에서나 투표할 수 있도록 하는 방식으로, 유권자들은 인터넷으로 연결된 단말기(PC)를 이용해 자신의 의사를 표시하며, 단말기를 떠난 투표 데이터는 네트워크를 통해 전송되어 서버에 저장된다.

<15> 국내외 여러 업체가 ASP(Application Service Provider) 형식의 상용 서비스를 시작한 대표적인 전자투표 방식으로, 인터넷뱅킹 또는 인터넷 전자상거래와 비슷한 개념의 방식이라 할 수 있다.

<16> 한편, TPM 기술은 보안 및 신뢰 서비스를 위해 저전력, 고성능의 하드웨어/소프트웨어 결합을 통한 신뢰 컴퓨팅 환경을 제공하는 것을 목적으로 하고 있다. TPM은 플랫폼 무결성 보증, 안전한 스토리지 제공 및 공통 암호 라이브러리를 지원한다.

<17> 여기서, 신뢰 컴퓨팅에 대한 선업 표준화를 목적으로 하는 단체인 TCG(Trusted Computing Group)는 TCPA(Trusted Computing Platform Alliance)의 후신으로 현재 세계 120 여개 회사가 참여하고 있는 표준화 단체이다. 신뢰 컴퓨팅은 사용자 정보와 컴퓨팅 환경을 보호하고, 암호키를 통한 하드웨어로 보호되는 애플리케이션을 제공하며, 안전한 플랫폼들 간의 상호 인증을 제공하는 것을 목적으로 한다.

<18> 상기 TPM은 TCG에 의해 정의된 하드웨어로, 컴퓨팅 플랫폼에 임베디드 형태로 장착되어 신뢰 근원(root of trust)의 역할을 한다.

<19> TPM은 암호키들을 생성, 사용 및 보호하고, 플랫폼이 동일한 configuration일 때에만 읽기 가능한 데이터를 암호화하는 이른바 "Sealed storage"를 제공한다.

<20> 또한, 플랫폼에 대한 측정값(Platform Configuration Register, 이하 PCR)을 저장하고 서명하는 방법으로 플랫폼 상의 소프트웨어를 측정한다.

<21> 그리고 본 발명과 연관된 기능으로서, 유효한 TPM 임을 인증하고 PCR 값에 대한 서명을 제공하는 방법으로 제삼자에 대한 PCR 값 보증 기능을 제공한다.

<22> 프라이빗-CA(privacy-Certificate Authority)을 이용한 보증은 보증 과정을 위해, 각 플랫폼의 TPM이 유일한 암호키(Endorsement Key, 이하 EK)를 갖고, 각 검증자는 유효한 TPM들의 EK를 알거나 인증기관이 발급한 각 EK에 대한 인증서를 가지고 있다.

<23> 플랫폼이 안전한 OS(Operating System)를 실행하는지 여부를 검증자가 알고자 할 경우, TPM은 유효한 TPM임을 검증자에게 보증하기 위해, 플랫폼에 대한 측정값(PCR 값)을 검증자에게 송신하고, 검증자는 EK를 통해 해당 PCR을 확인하여 TPM이 유효한지 여부를 검증한다.

<24> 그러나 위와 같은 방법에서는 두 개 이상의 검증자들이 동일한 플랫폼에서의 보증임을 알게 되고, 이를 통해 동일한 사용자의 동작들이 링크될 가능성이 있으므로 TPM이 장착된 플랫폼의 익명성을 보장할 수 없다는 문제점이 있다.

<25> 이 문제의 해결을 위해 제삼자인 사설 인증기관을 두어 검증자마다 다른 키를 사용할 수 있도록 한다. 각 플랫폼의 TPM이 EK외에 각 검증자마다의 보증키(Attestation Identity Key, 이하 AIK)를 갖도록 한다.

<26> AIKi는 RSA키쌍으로서 AIKi_공개키(검증키)와 AIKi_비밀키(서명키)로 구성된다. 이를 이용한 보증 과정은 다음과 같다.(이때, i는 $1 \leq i \leq k$, k는 검증자의 수)

<27> TPM은 EK와 AIKi_공개키를 사설 인증기관에게 보내고, 사설 인증기관은 EK가 유효한지 여부를 검사한다.

<28> 사설 인증기관으로부터 자신이 서명한 AIKi_공개키의 인증서인 $SIG_{privacy-CA}$(AIKi_공개키)를 EK로 암호화된 형태로 얻는다. (이때, SIGx(Y)는 X를 키로 하는 Y에 대한 서명)

<29> TPM은 복호화를 통해 $SIG_{privacy-CA}$(AIKi_공개키)를 얻는다.

<30> 검증자가 요청하면, TPM은 $SIG_{privacy-CA}$(AIKi_공개키)와 AIKi_공개키, 그리고 플랫폼을 측정한 값인 PCR을 AIKi_비밀키로 서명한 $SIG_{AIKi\_비밀키}$(PCR)와 플랫폼 측정 리스트(Measurement List, 이하 ML)를 검증자에게 포워딩한다.

<31> 검증자는 TPM으로부터 받은 인증서 $SIG_{privacy-CA}$(AIKi_공개키)를 통해 함께 수신한 AIKi_공개키를 확인한 후, 이 키를 통해 $SIG_{AIKi\_비밀키}$(PCR)를 검증하여 PCR을 획득한다.

<32> 그리고 함께 수신한 ML과 PCR의 내용을 비교하여 보증을 확인한다.

발명이 이루고자 하는 기술적 과제

<33> 이에 본 발명의 목적은 인터넷 전자투표를 구성하는 참여자인 유권자, 투표서버 및 개표서버 모두를 신뢰할 수 있도록 상호 보증(Mutual attestation) 기능을 추가하여 신뢰 플랫폼 상에서 각 참여자 모두가 전자투표 시스템을 믿고 이용할 수 있는 인터넷 전자투표 방법 및 시스템을 제공하는 데 있다.

<34> 또한 저전력, 고성능의 TPM 칩을 유권자(PC), 투표서버 및 개표서버의 메인 보드에 각각 장착하여 성능을 극대화하는 동시에, 기존의 공개키 기반구조 상의 인증기관이 사설 인증기관 역할을 하도록 하여 유권자와 서버들간의 상호 보증의 주체가 될 수 있도록 해주는 인터넷 전자투표 방법 및 시스템을 제공하는 데 있다.

발명의 구성 및 작용

<35> 상기한 목적을 달성하기 위한 본 발명에 따른 유권자 단말기, 투표서버, 개표서버, 및 인증서버를 참여자로 가지는 인터넷 전자투표 방법은, 유권자 단말기, 투표서버, 개표서버 및 인증서버를 참여자로 가지는 인터넷 전자투표 방법에 있어서, 상기 유권자 단말기, 투표서버 및 개표서버 각각은 TPM(Trusted Platform Module)을 이용하여 상기 인증서버로부터 자신의 인증서를 제공받고, 상기 투표서버와 상기 개표서버는 자신의 인증서를 서로 교환한 후 투표 처리 정보와 개표 처리 정보를 각각 생성하는 전처리 과정; 상기 유권자 단말기, 상기 투표서버 및 상기 개표서버가 상기 TPM을 이용하여 서로를 보증한 후, 상기 개표서버가 상기 유권자 단말기에서 생성된 투표횟수를 통해 이중 투표를 검사하고, 상기 유권자 단말기가 투표 정보를 생성하면, 상기 투표서버는 상기 투

표 처리 정보에 따라 상기 투표 정보를 저장하는 투표 과정; 및 상기 저장된 투표 정보를 상기 개표 처리 정보에 따라 분석하여 투표 내용을 집계하고 출력하는 개표 과정을 포함한다.

<36> 상기한 목적을 달성하기 위한 본 발명에 따른 인터넷 전자투표 시스템은, TPM(Trusted Platform Module)의 프라이버시-CA(Certificate Authority)으로써 인증 작업을 수행하는 인증서버; 상기 TPM을 이용하여 상기 인증서버와의 인증 작업과 하기의 투표서버 및 개표서버와의 상호 보증 작업을 수행한 후, 투표 작업을 수행하고, 투표 횟수를 생성하여 전송하는 유권자 단말기; 상기 TPM을 이용하여 상기 인증서버와의 인증 작업과 상기 유권자 단말기와의 상호 보증 작업을 수행한 후, 상기 유권자 단말기로부터 전송되는 투표정보를 저장하는 투표서버; 및 상기 TPM을 이용하여 상기 인증서버와의 인증 작업과 상기 유권자 단말기와의 상호 보증 작업을 수행한 후, 투표 시에는 상기 유권자 단말기에 상기 투표정보를 입력할 수 있도록 하는 투표 티켓을 제공하고, 개표 시에는 상기 유권자 단말기로부터 전송받은 상기 투표횟수를 통해 이중 투표를 검사하고, 상기 투표서버를 통해 저장된 상기 투표 정보를 분석하여 투표결과를 발표하는 개표서버를 포함한다.

<37> 이하, 본 발명에 따른 인터넷 전자투표 방법에 대한 바람직한 실시예에 대하여 첨부한 도면을 참조하여 상세하게 살펴보기로 한다. 이 때, 아래에서 설명하는 시스템 구성은 본 발명의 설명을 위해서 인용한 시스템으로써 아래 시스템으로 본 발명을 한정하지 않음을 이 분야의 통상의 지식을 가진 자라면 이해해야할 것이다.

<38> 도1은 본 발명의 일실시예에 따른 인터넷 전자투표 시스템의 구성을 나타낸 도면이다.

<39> 도1을 참조하면, 본 발명의 인터넷 전자투표 시스템은 유권자 단말기(100), 투표서버(200), 개표서버(300), 인증서버(400), 그리고 유권자 데이터베이스(500) 및 투표 데이터베이스(600)를 포함한다. 그리고 유권자 단말기(100), 투표서버(200), 및 개표서버(300) 각각에는 TPM이 장착된다.

<40> 유권자 단말기(100)는 TPM을 이용하여 인증서버(400)로부터 자신의 인증서(SIG_{CA}(AIK_Vi_공개키)를 제공받아 보유하고 있으며, 유권자(Vi)에 의해 투표 정보가 입력되면 유권자 TPM 정보를 첨부하여 투표서버(200) 및 개표서버(300)에 전송한 후, TPM을 이용한 보증 작업이 정상적으로 완료된 후에만 실질적인 투표 작업을 수행하도록 한다.

<41> 투표서버(200)는 TPM을 이용하여 인증서버(400)로부터 자신의 인증서(SIG_{CA}(AIK_투표서버_공개키)를 제공받고, 투표시에는 유권자 단말기(100)로부터 전송되는 유권자 TPM 정보를 이용하여 유권자 단말기(100)를 보증한 후, 투표 정보를 투표 데이터베이스(600)에 저장한다. 그리고 개표 시에는 투표 데이터베이스(600)에 저장된 투표 정보들을 개표서버(300)에 제공해준다.

<42> 개표서버(300)는 TPM을 이용하여 인증서버(400)로부터 자신의 인증서(SIG_{CA}(AIK_개표서버_공개키)를 제공받고, 투표시에는 유권자 단말기(100)로부터 전송되는 유권자 TPM 정보를 이용하여 유권자 단말기(100)를 보증한 후, 투표 정보를 생성할 수 있는 투표 티켓(T)을 제공한다. 그리고 개표 동작시에는 투표서버(200)가 제공하는 투표 정보를 분석하여, 투표 결과를 발표한다.

<43> 인증서버(400)는 TPM의 사설 인증기관으로서의 기능을 수행하여, 플랫폼의 익명성을 제공하면서 유권자 단말기(100), 투표서버(200), 개표서버(300) 각각에 대한 인증을 수행한 후, 각각의 인증서를 제공한다.

<44> 유권자 데이터베이스(500)는 투표와 관련된 유권자 단말기(또는 유권자)(100)의 모든 정보를 저장하고, 투표 데이터베이스(600)는 투표서버(200)에 의해 저장되는 투표 정보들이 저장된다.

<45> 이하에서는 본 발명의 일실시예에 따른 인터넷 전자투표 방법을 설명하기로 한다.

<46> 도2는 인터넷 전자투표 방법의 전처리 과정을 설명하기 위한 도면이고, 도3a 및 도3b는 투표 과정을 설명하기 위한 도면이고, 도4는 개표 과정을 설명하기 위한 도면이다.

<47> 도2를 참조하여, 인터넷 전자투표 시스템의 투표 및 개표를 위한 전처리 과정을 설명하면 다음과 같다.

<48> 먼저, 유권자 단말기(100), 투표서버(200), 및 개표서버(300)가 보증에 관한 인증서를 발급받기 위해 자신의 EK와 AIK를 인증서버(400)에 전송한다(S110).

<49> 단계 S110에서, 유권자 단말기(100)는 EK_Vi와 AIK_Vi_공개키(이때, Vi는 유권자 단말기의 식별 번호)를, 투표서버(200)는 EK_투표서버와 AIK_투표서버_공개키를, 개표서버(300)는 EK_개표서버와 AIK_개표서버_공개키를 인증서버(400)로 각각 전송한다.

<50> 인증서버(400)는 수신한 EK_Vi, EK_투표서버, EK_개표서버 각각을 이용하여 유권자 단말기(100), 투표서버

(200), 및 개표서버(300)의 유효성을 검사한 후, 자신이 서명한 AIK_공개키의 인증서인 SIG_{CA}(AIK_Vi_공개키), SIG_{CA}(AIK_투표서버_공개키), SIG_{CA}(AIK_개표서버_공개키)를 대응되는 EK로 암호화하여 유권자 단말기(100), 투표서버(200), 및 개표서버(300) 각각으로 제공한다(S120).

<51> 그러면, 투표서버(200)와 개표서버(300)는 자신의 인증서인 SIG_{CA}(AIK_투표서버_공개키)와 SIG_{CA}(AIK_개표서버_공개키)를 개표 과정 시에 사용하기 위해 상호 교환한다(S130).

<52> 그리고 투표서버(200)는 유권자수 만큼(N개)의 무작위 수열을 생성하고(S140), 개표서버(300)는 유권자수 만큼(N개)의 무작위 수열을 생성함과 동시에 k 종류의 투표 티켓(T)을 유권자수 만큼(N개) 생성하고, 이를 섞는다(S150).

<53> 이때, 투표서버(200) 및 개표서버(300)는 생성된 무작위 수열을 외부에는 비밀로 한다.

<54> 도2의 방법이 완료되면, 도3a 및 도3b에서와 같이 투표 과정을 진행된다.

<55> 먼저, 단계 S211에서는 임의의 유권자 단말기(100)를 통해 유권자가 전자투표를 하면, 유권자 단말기(100)는 제1난수(f1), 투표횟수(RN), 투표횟수(RN)에 대한 해쉬값(H(RN)), 투표시간(TS)을 생성하고, 이를 유권자 TPM 정보와 함께 투표서버(200)와 개표서버(300)에 각각 전송한다.

<56> 이때, 유권자 TPM 정보는 SIG_{CA}(AIK_Vi_공개키), AIK_Vi_공개키, 그리고 PCR을 EK_Vi로 서명한 서명값(S)과 ML로 이루어지며, 서명값(S)은 수학식1에 따라 생성된다.

수학식 1

<57> $S=SIG_{AIK\_Vi\_비밀키}(H(RN) \| TS \| PCR)$

<58> 단계 S212에서, 투표서버(200) 및 개표서버(300) 각각은 유권자 단말기(100)가 전송하는 유권자 TPM 정보를 이용하여 유권자에 대한 보증 작업을 수행하고, 투표횟수(RN)를 이용하여 이중 투표 검사 작업을 수행한 후, 유권자 단말기(100)가 자신을 신뢰할 수 있도록 TPM 정보를 생성하여 유권자 단말기(100)에 각각 전송한다. 단계 S212에 대한 상세한 설명은 이하의 도5a 및 도5b를 통해 보다 상세히 설명하기로 한다.

<59> 여기서, 투표서버 TPM 정보는 SIG_{CA}(AIK_투표서버_공개키), AIK_투표서버_공개키, 그리고 PCR을 투표서버(200)의 AIK_개표서버_비밀키로 서명한 서명값($SIG_{AIK\_투표서버\_비밀키}$(PCR))과 ML로 이루어지고, 개표서버 TPM 정보는 SIG_{CA}(AIK_개표서버_공개키)와 AIK_개표서버_공개키, 그리고 PCR을 개표서버(300)의 AIK_개표서버_비밀키로 서명한 서명값($SIG_{AIK\_개표서버\_비밀키}$(PCR))과 ML로 이루어진다.

<60> 단계 S213에서, 유권자 단말기(100)는 투표서버 TPM 정보와 개표서버 TPM 정보를 통해 투표서버(200) 및 개표서버(300)의 신뢰성을 확인한다.

<61> 이를 위해, 유권자 단말기(100)는 투표서버(200)로부터 받은 SIG_{CA}(AIK_개표서버_공개키)을 통해 함께 수신한 AIK_투표서버_공개키를 확인하고, 이 키를 통해 투표서버(200)의 서명값($SIG_{AIK\_개표서버\_비밀키}$(PCR))을 검증하여 PCR을 획득한 후, 함께 수신한 ML과 PCR의 내용을 비교하여 보증을 확인한다. 그리고 개표서버(300)의 신뢰성도 이와 동일한 방법으로 확인한다.

<62> 단계 S214에서, 개표서버(300)가 제2 난수(f2)를 생성한 후, 수학식2에 따라 유권자 단말기(100) AIK_Vi_공개키로 암호화하여 유권자 단말기(100)로 전송한다.

수학식 2

<63> $A = ENC_{AIK\_Vi\_공개키}(f2)$

<64> 여기서, ENCx(Y)는 X를 키로 하는 Y에 대한 공개키 암호화 함수이다.

<65> 단계 S215에서, 유권자 단말기(100)는 암호화된 제2 난수(A)를 복호화하여 제2 난수(f2)를 획득하고, 이를 자신이 생성해놓은 제1 난수(f1)를 통해 다시 암호화하여 개표서버(300)에게 전송한다.

수학식 3

<66> $f2 = DEC_{AIK\_Vi\_비밀키}(A)$,

<67> $B = E_{f2}(f1)$

<68> 여기서, DECx(Y)는 X를 키로 하는 Y에 대한 공개키 복호화 함수이고, Ex(Y)는 X를 키로 하는 Y에 대한 대칭키 암호화 함수이다.

<69> 단계 S216에서, 유권자 단말기(100)는 제1 난수(f1)와 제2 난수(f2)를 배타적 논리합(XOR)하여 개표서버(400)와의 세션키(SK_Vi개표)를 생성한다.

수학식 4

<70> SK_Vi개표 = f1 XOR f2

<71> 단계 S217에서, 개표서버(400)는 암호화된 제2 난수(B)로부터 제1 난수(f1)를 추출하고 유권자 단말기(100)와의 세션키(SK_Vi 개표)를 획득한 후, 세션키(SK_Vi 개표)를 이용하여 투표 티켓(T)을 암호화하여 유권자 단말기(100)로 전송한다.

수학식 5

<72> $C = E_{SK\_Vi\ 개표}(T)$

<73> 단계 S218에서, 유권자 단말기(100)는 자신의 세션키(SK_Vi 개표)를 이용해 암호화된 투표 티켓(C)을 복호화하여 투표 티켓(T)을 획득한 후, 이에 투표내용(O) 및 자신의 비밀번호(PW)를 기입하여 수학식 6에 따라 투표값(p)을 생성한다. 그리고 자신의 EK_Vi로 서명하여 유권자 서명값(r)을 더 생성한 후, 투표값(p)과 유권자 서명값(r)을 함께 투표서버(300)에게 전송한다.

수학식 6

<74> $p = ENC_{AIK\_투표서버\_공개키}(T \,||\, O \,||\, PW)$,

<75> $r = SIG_{AIK\_Vi\_비밀키}(p)$

<76> 단계 S219에서, 투표서버(300)는 투표값(p)과 유권자 서명값(r)을 수신하여 유권자 서명값(r)을 검증한 후, 유권자 데이터베이스(500)에 인증서 일련번호, 인증서 발급기관, SIG_{CA}(AIK_Vi_공개키), 투표시간(TS), 유권자 단말기의 링크 주소(URL), 및 서명값(S)을 포함하는 유권자 단말기(또는 유권자)의 정보를 저장한다. 그리고 투표값(p)을 수학식7에 따라 AIK_투표서버_비밀키로 서명하여 투표서버 서명값(q)로 변환한 후, 유권자 단말기(100)에게 전송한다.

수학식 7

<77> $q = SIG_{AIK\_투표서버\_비밀키}(p)$

<78> 단계 S210에서, 유권자 단말기(100)는 투표서버 서명값(q)을 검증한 후 자신이 투표한 값(p)이 성공적으로 전달되었음을 개표서버(300)에 통보하기 위해, 투표횟수(RN)를 개표서버(400)와의 세션키(SK_Vi 개표)로 암호화하여 개표서버(300)에게 전송한다.

수학식 8

<79> $D = E_{SK\_Vi\ 개표}(RN)$

<80> 단계 S211에서, 개표서버(400)는 암호화된 세션키($E_{SK\_Vi\ 개표}(RN)$)를 자신의 세션키(SK_Vi 개표)로 복호화하여 투표횟수(RN)를 추출한 후, 유권자 데이터베이스(500)에 저장된 값들을 참조하여 올바른 투표횟수(RN)가 전송되었는지를 확인함과 동시에 투표서버(300)가 유권자 데이터베이스(500)에 값들을 올바르게 기록하였는지 검사한다. 검사가 성공하면, 이에 대한 투표횟수(RN)에 대한 해쉬값(H(RN+1))을 유권자 단말기(100)에게 전송하여 이를 통보하고, 투표횟수(RN)를 유권자 데이터베이스(500)에 기록한다.

<81> 단계 S212에서, 유권자 단말기(100)는 수신된 해쉬값(H(RN+1))과 자신의 투표횟수(RN)를 비교하여 투표의 정상

수행 여부를 확인한 후, 투표가 정상적으로 완료되었다는 의미로 해쉬값(H(RN+2))을 투표서버(300)에 전송한다.

<82> 단계 S213에서, 투표서버(300)는 해쉬값 H(RN+2)를 받아 유권자 데이터베이스(500)에 기록된 투표횟수(RN)와 비교하여 올바른 값인지 검증하고, 검증이 성공하면 투표 종료를 유권자 단말기(100)에게 알리고, 투표값 및 개표서버의 서명값쌍(p, r)에 미리 생성해 놓은 무작위 수열을 매핑하여 투표 데이터베이스(600)에 저장한다.

<83> 이와 같은 도3a 및 도3b의 투표 과정이 완료되면, 마지막은 도4에서와 같이 개표 과정을 진행된다.

<84> 단계 S310에서, 투표서버(200)가 투표 종료 후 무작위 수열에 따라 투표값 및 개표서버의 서명값쌍(p, r)을 정렬한 후, 투표 데이터베이스(600)에 기재된 숫자를 지우고 이를 개표서버(300)에게 전달한다.

<85> 단계 S320에서, 개표서버(300)가 투표 데이터베이스(600)를 받아 무작위 수열을 투표값 및 개표서버의 서명값쌍(p, r)에 부여하고 이를 정렬한다.

<86> 단계 S330에서, 개표서버(300)가 투표 데이터베이스(600)를 공개 및 개표하고 투표 마감자수와 투표 데이터베이스(600)의 투표수가 일치하는지를 검사한 후, 수학식9에 따라 각각의 투표값 및 개표서버의 서명값쌍(p, r)에 대하여 투표서버 서명값(q)의 서명을 검증한다.

수학식 9

<87> $VER_{AIK\_투표서버\_공개키}(q, p)$

<88> 여기서, $VER_X(Y,Z)$는 키 X를 통해 서명 Y를 풀고, 이 결과 값을 Z와 비교하는 검증하는 함수이다.

<89> 단계 S340에서, 개표서버(300)는 수학식10에 따라 투표값(p)을 자신의 AIK_개표서버_비밀키로 복호화하여 투표내용(O), 투표 티켓(T), 비밀 번호(PW)등을 획득한다.

수학식 10

<90> $(T \| O \| PW)=DECAIK_{\_개표서버\_비밀키}(p)$

<91> 단계 S350에서, 개표서버(300)는 투표 티켓(T)이 발행 내용을 통해 올바른 투표 티켓이 포함되었는지 그리고 개수가 일치하는지를 검사하고, 투표내용을 집계한 후, 이를 발표하고 검증 자료로서 투표내용(O), 투표 티켓(T), 비밀 번호(PW)를 공개한다.

<92> 이하의 도5a 및 도5b는 도3의 단계 S212를 보다 상세히 설명하기 위한 흐름도로, 도5a는 투표서버의 보증 동작을, 도5b는 개표서버의 보증 동작을 각각 나타낸다.

<93> 먼저, 도5a를 참조하여 단계 S212에서의 투표서버의 동작을 설명하기로 한다.

<94> 투표서버(200)는 유권자 단말기(100)부터 받은 SIG_{CA}(AIK_Vi_공개키)를 통해 함께 수신한 AIK_Vi_공개키를 확인한다(S2121).

<95> 그리고 AIK_Vi_공개키를 통해 $SIG_{AIK\_Vi\_비밀키}$(H(RN)||TS||PCR)를 검증하여 PCR을 획득한 후(S2122), 수신한 ML과 PCR의 내용을 비교하여 보증을 확인한다(S2123).

<96> 이어서, 유권자 데이터베이스(500)의 항목을 조사하여 투표횟수(RN)의 존재 여부를 확인하여 이중 투표 여부를 검사한다(S2124).

<97> 단계 S2124의 검사 결과, 유권자 데이터베이스(500)에 동일한 투표횟수(RN)가 이미 존재하면, 투표서버(200)는 해당 유권자(Vi)가 이중 투표임을 알린 후 투표를 종료하고, 그렇지 않으면 다음의 단계 S213을 진행한다.

<98> 계속하여, 도5b를 참조하여 단계 S212에서의 개표서버의 동작을 설명하기로 한다.

<99> 개표서버(300)는 유권자(Vi)부터 받은 SIG_{CA}(AIK_Vi_공개키)를 통해 함께 수신한 AIK_Vi_공개키를 확인한다(S2126).

<100> 그리고 AIK_Vi_공개키를 통해 $SIG_{AIK\_Vi\_비밀키}$(H(RN)||TS||PCR)를 검증하여 PCR을 획득한 후(S2127), 개표서버(300)가 함께 수신한 ML과 PCR의 내용을 비교하여 보증을 확인한다(S2128).

<101> 그리고 유권자 데이터베이스(500)의 항목을 조사하여 투표횟수(RN)의 존재 여부를 확인하여 이중 투표 여부를

검사한다(S2129).

<102> 단계 S2129의 검사 결과, 유권자 데이터베이스(500)에 동일한 투표횟수(RN)가 이미 존재하면, 개표서버(300)는 해당 유권자(Vi)가 이중 투표임을 알린 후 투표를 종료하고, 그렇지 않으면 다음의 단계 S213을 진행한다.

<103> 즉, 본 발명의 투표서버와 개표서버는 TPM을 이용하여 동일한 방법으로 유권자에 대한 보증 작업과 이중 투표 검사 작업을 수행한다.

<104> 이상에서 설명한 본 발명은 전술한 실시 예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경할 수 있다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 당업자에게 있어 명백할 것이다.

발명의 효과

<105> 상술한 바와 같이 본 발명에 의한 인터넷 전자투표 방법 및 시스템에 의하면, 저전력, 고성능의 TPM을 인터넷 전자투표의 구성 요소인 유권자 단말기, 투표서버 및 개표서버에 각각 장착하여 성능을 극대화하는 동시에 기존의 공개키 기반 구조상의 인증기관이 사설 인증기관 기능을 하도록 하여 유권자 단말기와 서버들간 보증 주체가 될 수 있도록 하여, 투표 참여자인 유권자와 해당 서버들이 상호 보증을 통해 서로 신뢰를 확인한 후 안심하고 투표할 수 있도록 해주는 뛰어난 효과가 있다.

도면의 간단한 설명

<1> 도1은 본 발명의 일실시예에 따른 인터넷 전자투표 시스템의 구성을 나타낸 도면,

<2> 도2는 본 발명의 일실시예에 따른 인터넷 전자투표 방법의 전처리 과정을 설명하기 위한 도면,

<3> 도3a 및 도3b는 본 발명의 일실시예에 따른 인터넷 전자투표 방법의 투표 과정을 설명하기 위한 도면,

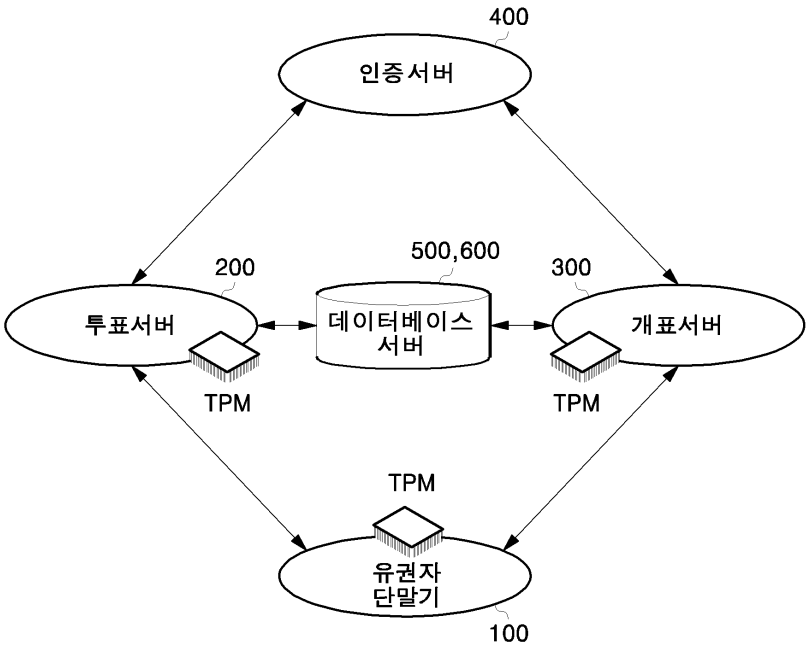
<4> 도4는 본 발명의 일실시예에 따른 인터넷 전자투표 방법의 개표 과정을 설명하기 위한 도면,

<5> 도5a는 본 발명의 일실시예에 따른 투표서버의 보증 과정을 보다 상세히 설명하기 위한 도면, 그리고

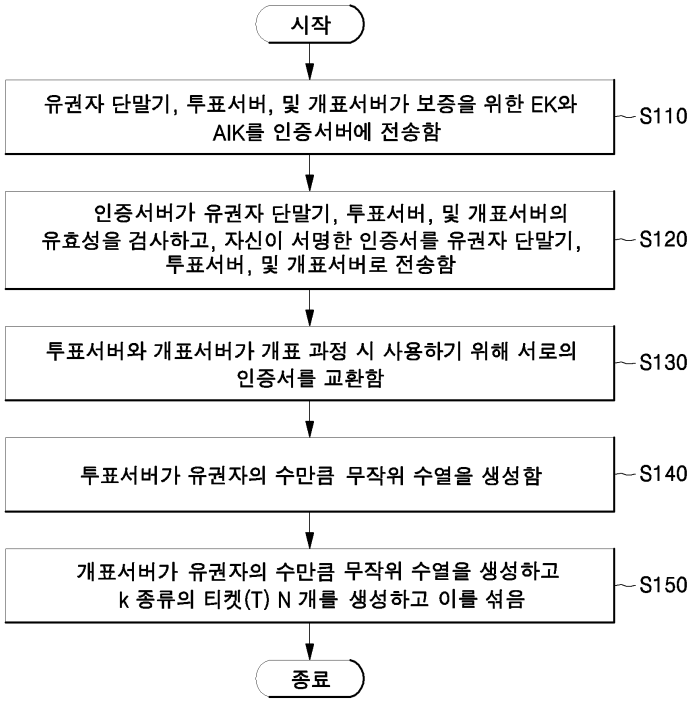
<6> 도5a는 본 발명의 일실시예에 따른 개표서버의 보증 과정을 보다 상세히 설명하기 위한 도면이다.

도면

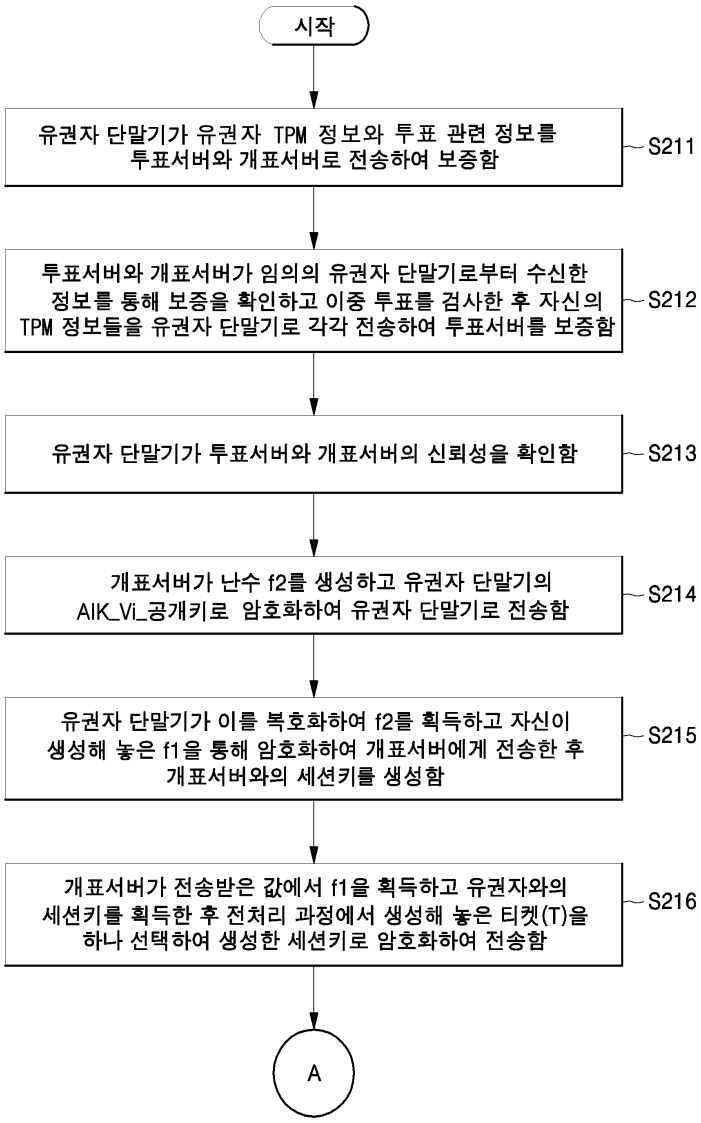
도면1



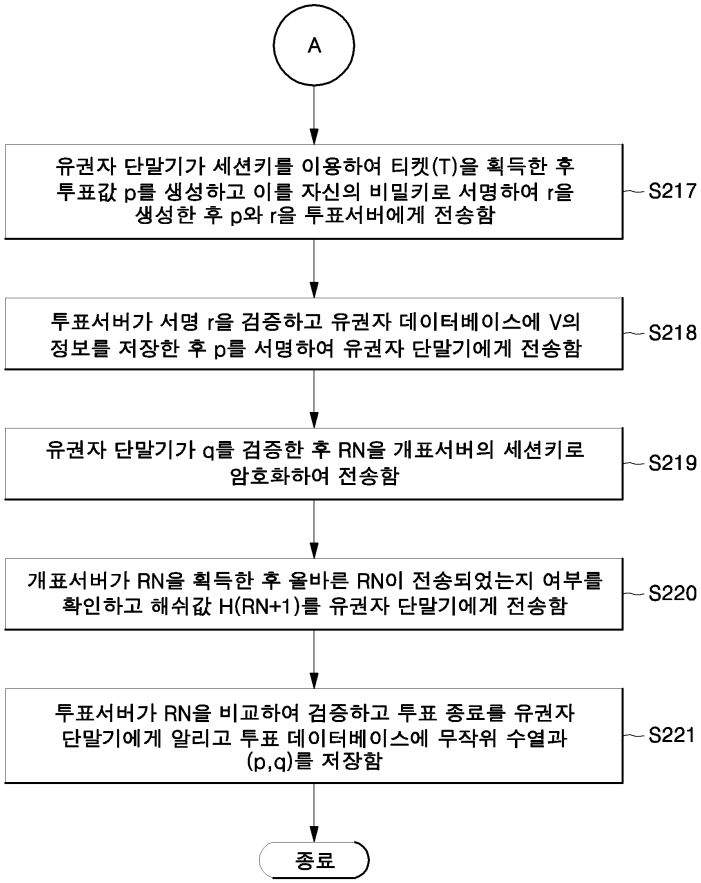
도면2


시작
유권자 단말기, 투표서버, 및 개표서버가 보증을 위한 EK와 AIK를 인증서버에 전송함
S110
인증서버가 유권자 단말기, 투표서버, 및 개표서버의 유효성을 검사하고, 자신이 서명한 인증서를 유권자 단말기, 투표서버, 및 개표서버로 전송함
S120
투표서버와 개표서버가 개표 과정 시 사용하기 위해 서로의 인증서를 교환함
S130
투표서버가 유권자의 수만큼 무작위 수열을 생성함
S140
개표서버가 유권자의 수만큼 무작위 수열을 생성하고 k 종류의 티켓(T) N 개를 생성하고 이를 섞음
S150
종료

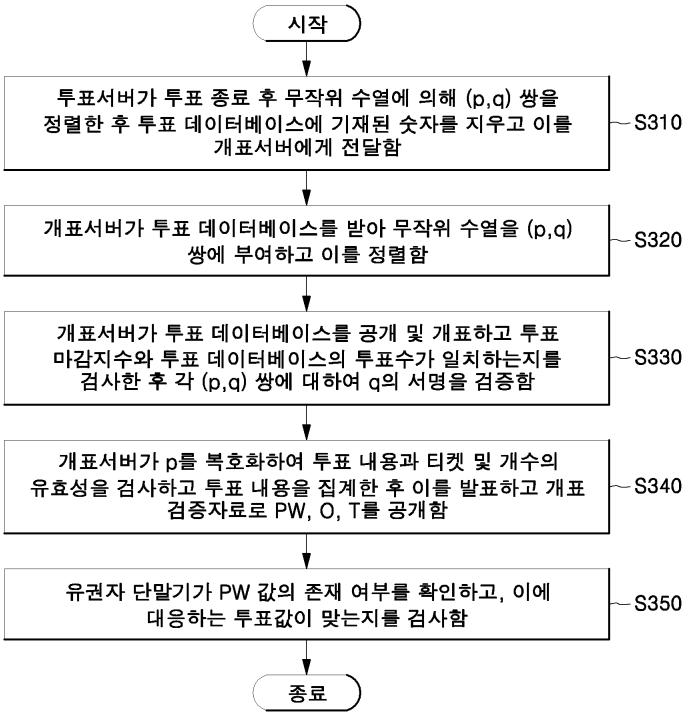
도면3a


시작
유권자 단말기가 유권자 TPM 정보와 투표 관련 정보를 투표서버와 개표서버로 전송하여 보증함
S211
투표서버와 개표서버가 임의의 유권자 단말기로부터 수신한 정보를 통해 보증을 확인하고 이중 투표를 검사한 후 자신의 TPM 정보들을 유권자 단말기로 각각 전송하여 투표서버를 보증함
S212
유권자 단말기가 투표서버와 개표서버의 신뢰성을 확인함
S213
개표서버가 난수 f2를 생성하고 유권자 단말기의 AIK_Vi_공개키로 암호화하여 유권자 단말기로 전송함
S214
유권자 단말기가 이를 복호화하여 f2를 획득하고 자신이 생성해 놓은 f1을 통해 암호화하여 개표서버에게 전송한 후 개표서버와의 세션키를 생성함
S215
개표서버가 전송받은 값에서 f1을 획득하고 유권자와의 세션키를 획득한 후 전처리 과정에서 생성해 놓은 티켓(T)을 하나 선택하여 생성한 세션키로 암호화하여 전송함
S216
A

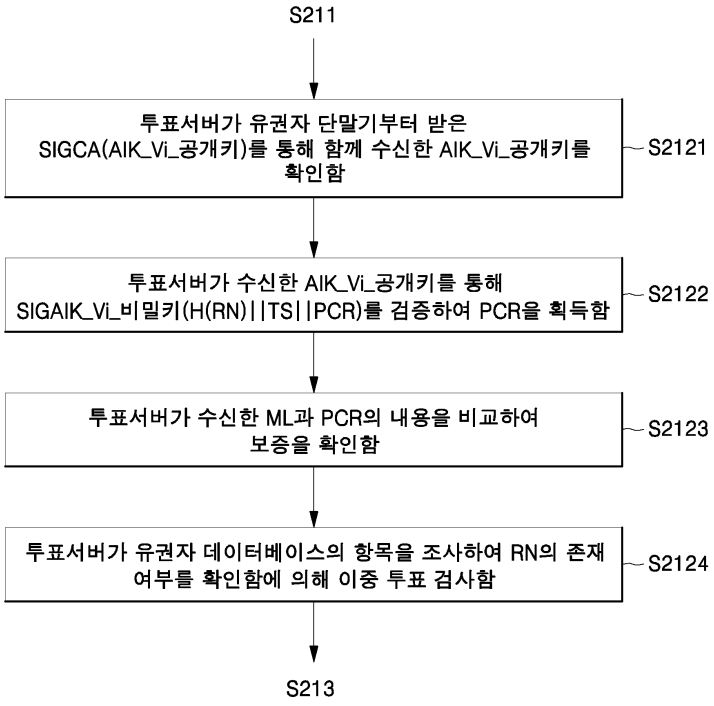
도면3b


A
유권자 단말기가 세션키를 이용하여 티켓(T)을 획득한 후 투표값 p를 생성하고 이를 자신의 비밀키로 서명하여 r을 생성한 후 p와 r을 투표서버에게 전송함
S217
투표서버가 서명 r을 검증하고 유권자 데이터베이스에 V의 정보를 저장한 후 p를 서명하여 유권자 단말기에게 전송함
S218
유권자 단말기가 q를 검증한 후 RN을 개표서버의 세션키로 암호화하여 전송함
S219
개표서버가 RN을 획득한 후 올바른 RN이 전송되었는지 여부를 확인하고 해쉬값 H(RN+1)를 유권자 단말기에게 전송함
S220
투표서버가 RN을 비교하여 검증하고 투표 종료를 유권자 단말기에게 알리고 투표 데이터베이스에 무작위 수열과 (p,q)를 저장함
S221
종료

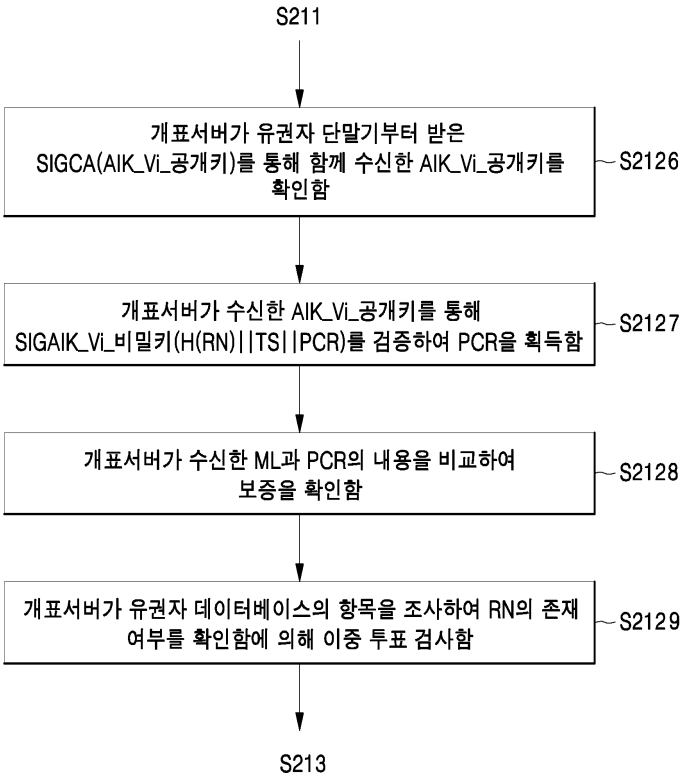
도면4


시작
투표서버가 투표 종료 후 무작위 수열에 의해 (p,q) 쌍을 정렬한 후 투표 데이터베이스에 기재된 숫자를 지우고 이를 개표서버에게 전달함
S310
개표서버가 투표 데이터베이스를 받아 무작위 수열을 (p,q) 쌍에 부여하고 이를 정렬함
S320
개표서버가 투표 데이터베이스를 공개 및 개표하고 투표 마감지수와 투표 데이터베이스의 투표수가 일치하는지를 검사한 후 각 (p,q) 쌍에 대하여 q의 서명을 검증함
S330
개표서버가 p를 복호화하여 투표 내용과 티켓 및 개수의 유효성을 검사하고 투표 내용을 집계한 후 이를 발표하고 개표 검증자료로 PW, O, T를 공개함
S340
유권자 단말기가 PW 값의 존재 여부를 확인하고, 이에 대응하는 투표값이 맞는지를 검사함
S350
종료

도면5a


S211
투표서버가 유권자 단말기부터 받은 SIGCA(AIK_Vi_공개키)를 통해 함께 수신한 AIK_Vi_공개키를 확인함
S2121
투표서버가 수신한 AIK_Vi_공개키를 통해 SIGAIK_Vi_비밀키(H(RN)||TS||PCR)를 검증하여 PCR을 획득함
S2122
투표서버가 수신한 ML과 PCR의 내용을 비교하여 보증을 확인함
S2123
투표서버가 유권자 데이터베이스의 항목을 조사하여 RN의 존재 여부를 확인함에 의해 이중 투표 검사함
S2124
S213

도면5b


S211
개표서버가 유권자 단말기부터 받은 SIGCA(AIK_Vi_공개키)를 통해 함께 수신한 AIK_Vi_공개키를 확인함
S2126
개표서버가 수신한 AIK_Vi_공개키를 통해 SIGAIK_Vi_비밀키(H(RN)||TS||PCR)를 검증하여 PCR을 획득함
S2127
개표서버가 수신한 ML과 PCR의 내용을 비교하여 보증을 확인함
S2128
개표서버가 유권자 데이터베이스의 항목을 조사하여 RN의 존재 여부를 확인함에 의해 이중 투표 검사함
S2129
S213