



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0146730
(43) 공개일자 2024년10월08일

- (51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) G06Q 50/26 (2024.01)
H04L 9/08 (2006.01)
- (52) CPC특허분류
H04L 9/3218 (2013.01)
G06Q 50/26 (2024.01)
- (21) 출원번호 10-2023-0041672
(22) 출원일자 2023년03월30일
심사청구일자 2023년03월30일
- (71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
- (72) 발명자
박종환
서울특별시 종로구 홍지문 2길 20 (홍지동, 상명대학교)
- (74) 대리인
김효승
경기도 수원시 장안구 덕영대로417번길 18, 101호
김효승
서울특별시 동대문구 답십리로56길 105, 102동 1802호
- (74) 대리인
김등용

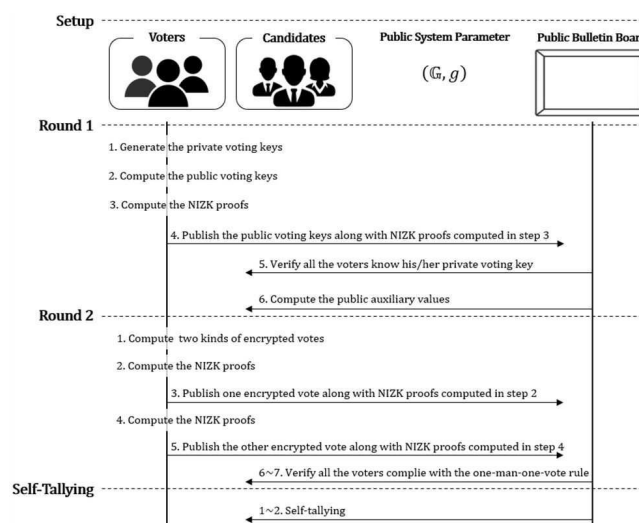
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 후보가 다수인 환경에서 효율적으로 동작하는 탈중앙 전자투표 시스템

(57) 요약

후보가 다수인 환경에서 효율적으로 동작하는 탈중앙 전자투표 시스템 및 방법이 개시된다. 상기 전자투표 방법은 유권자의 단말에 의해 수행되는 전자투표 방법으로, 소수(p)에 대한 군(G)와 상기 군(G)의 생성자(g)에 대한 (G, g)에 대하여 합의하는 단계, 비밀 투표키와 공개 투표키를 생성하고 상기 공개 투표키를 공개하는 단계, 복수의 후보들에 대한 암호화된 행사표와 암호화된 증명표를 생성하는 단계, 상기 암호화된 행사표를 공개하는 단계, 상기 암호화된 증명표를 공개하는 단계, 및 모든 유권자들의 행사표에 기초하여 복수의 후보들 각각에 대한 찬성표의 개수를 계산하는 단계를 포함한다.

대표도 - 도1



(52) CPC특허분류

H04L 9/0825 (2013.01)

H04L 9/3236 (2013.01)

G06Q 2230/00 (2013.01)

H04L 2209/463 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711194271
과제번호	2021-0-00518-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터경제를위한블록체인기술개발
연구과제명	블록체인 데이터 암호화 기반의 프라이버시 보호 기술개발
기 여 율	1/1
과제수행기관명	한양대학교산학협력단
연구기간	2023.01.01 ~ 2023.12.31

명세서

청구범위

청구항 1

유권자의 단말에 의해 수행되는 전자투표 방법에 있어서,
 소수(p)에 대한 군(G)와 상기 군(G)의 생성자(g)에 대한 (G,g)에 대하여 합의하는 단계;
 비밀 투표키와 공개 투표키를 생성하고 상기 공개 투표키를 공개하는 단계;
 복수의 후보들에 대한 암호화된 행사표와 암호화된 증명표를 생성하는 단계;
 상기 암호화된 행사표를 공개하는 단계;
 상기 암호화된 증명표를 공개하는 단계; 및
 모든 유권자들의 행사표에 기초하여 복수의 후보들 각각에 대한 찬성표의 개수를 계산하는 단계를 포함하는,
 전자투표 방법.

청구항 2

제1항에 있어서,
 k(k는 2 이상의 자연수) 명의 상기 복수의 후보들 중 i(i는 k 보다 작거나 같은 자연수) 번째 후보에 대한, 상기 모든 유권자들 중 l(l은 임의의 자연수) 번째 유권자인 상기 유권자의 상기 비밀 투표키는 $x_{l,i} \in \mathbb{Z}_p$ 이고,
 상기 공개 투표키는 $X_{l,i} = g^{x_{l,i}}$ 인,
 전자투표 방법.

청구항 3

제2항에 있어서,
 상기 공개하는 단계는,
 모든 i에 대해 상기 비밀 투표키를 알고 있다는 사실을 제1 비대화형 영지식(non-interactive zero-knowledge, NIZK) 증명을 이용하여 증명하는 단계를 포함하는,
 상기 공개하는 단계는 상기 제1 NIZK의 제1 증명 값을 더 공개하는,
 전자투표 방법.

청구항 4

제3항에 있어서,
 상기 제1 증명값($\pi_{1,li} = (s, c)$)은,
 임의의 $r \in \mathbb{Z}_p$ 를 선택하는 과정,
 $a = g^r$ 를 계산하는 과정,
 암호학적 해시 함수(H)를 이용하여 $c = H(i \parallel g \parallel X_{l,i} \parallel a)$ 를 계산하는 과정,
 $s = r - x_{l,i}c$ 를 계산하는 과정, 및

상기 제1 증명 값을 $\pi_{1,li} = (s, c)$ 로 설정하는 과정을 통해 생성되는,
전자투표 방법.

청구항 5

제4항에 있어서,

상기 공개하는 단계 이후에,

상기 유권자를 제외한 모든 유권자의 제1 증명 값의 유효성을 검증하는 단계를 더 포함하고,

상기 제1 증명 값의 유효성을 검증하는 단계는 $c = H(i \parallel g \parallel X_{j,i} \parallel g^s X_{j,i}^c)$ 의 성립 여부를 판단하는,
전자투표 방법.

청구항 6

제5항에 있어서,

상기 제1 증명 값의 유효성을 검증하는 단계 이후에,

$$Y_{l,i} = \begin{cases} 1 / \prod_{j=2}^n X_{j,i} & (l=1), \\ \prod_{j=1}^{l-1} X_{j,i} / \prod_{j=l+1}^n X_{j,i} & (2 \leq l \leq n-1), \\ \prod_{j=1}^{n-1} X_{j,i} & (l=n). \end{cases}, \text{ 및}$$

$$Z_{l,i} = \begin{cases} 1 / \prod_{j=2}^k X_{l,j} & (i=1), \\ \prod_{j=1}^{i-1} X_{l,j} / \prod_{j=i+1}^k X_{l,j} & (2 \leq i \leq k-1), \\ \prod_{j=1}^{k-1} X_{l,j} & (i=k). \end{cases} \text{를 계산하는 단계를 더 포함하는,}$$

전자투표 방법.

청구항 7

제6항에 있어서,

상기 암호화된 행사표는 $U_{l,i} = Y_{l,i}^{x_{l,i}} g^{v_{l,i}}$ 이고,

상기 암호화된 증명표는 $V_{l,i} = Z_{l,i}^{x_{l,i}} g^{v_{l,i}}$ 인,

전자투표 방법.

청구항 8

제7항에 있어서,

상기 암호화된 행사표를 공개하는 단계는,

$U_{l,i}$ 를 계산하는 데에 사용한 $v_{l,i}$ 가 0 또는 1이라는 사실을 증명하기 위한 제2 비대화식 영지식 증명의 제2 증명 값을 더 공개하는,

전자투표 방법.

청구항 9

제8항에 있어서,

상기 제2 증명 값은,

$v_{l,i}=1$ 일 경우, 임의의 $r, s_1, d_1 \in \mathbb{Z}_p$ 를 선택하고, $a_1 = g^{s_1} X_{l,i}^{d_1}$ 과 $b_1 = Y_{l,i}^{s_1} U_{l,i}^{d_1}$ 을 계산하고, $a_2 = g^r$ 과 $b_2 = Y_{l,i}^r$ 을 계산하고, 암호학적 해시 함수 H 를 이용하여 $c = H(l \parallel g \parallel X_{l,i} \parallel U_{l,i} \parallel a_1 \parallel b_1 \parallel a_2 \parallel b_2)$ 를 계산하고, $d_2 = c - d_1$ 와 $s_2 = r - x_{l,i} d_2$ 을 계산하고,

$v_{l,i}=0$ 일 경우, 임의의 $r, s_2, d_2 \in \mathbb{Z}_p$ 를 선택하고, $a_1 = g^r$ 과 $b_1 = Y_{l,i}^r$ 을 계산하고, $a_2 = g^{s_2} X_{l,i}^{d_2}$ 과 $b_2 = Y_{l,i}^{s_2} (U_{l,i}/g)^{d_2}$ 을 계산하고, 암호학적 해시 함수 H 를 이용하여 $c = H(l \parallel g \parallel X_{l,i} \parallel U_{l,i} \parallel a_1 \parallel b_1 \parallel a_2 \parallel b_2)$ 를 계산하고, $d_1 = c - d_2$ 와 $s_1 = r - x_{l,i} d_1$ 을 계산하여,

상기 제2 증명 값($\pi_{2,li} = (s_1, s_2, d_1, d_2)$)을 생성하는,

전자투표 방법.

청구항 10

제9항에 있어서,

상기 암호화된 증명표를 공개하는 단계는 상기 암호화된 행사표와 상기 암호화된 증명표를 계산하는 데에 동일한 상기 비밀 투표키와 행사표를 사용하였다는 사실을 증명하기 위한 제3 비대화식 영지식 증명의 제3 증명 값을 더 공개하는,

전자투표 방법.

청구항 11

제10항에 있어서,

상기 제3 증명 값은,

임의의 $r_1, r_2 \in \mathbb{Z}_p$ 를 선택하는 과정,

$a = Y^{r_1} g^{r_2}$ 와 $b = Z^{r_1} g^{r_2}$ 를 계산하는 과정,

암호학적 해시 함수 H 를 이용하여 $c = H(l \parallel g \parallel U_{l,i} \parallel V_{l,i} \parallel a \parallel b)$ 를 계산하는 과정, 및

상기 제3 증명 값을 $\pi_{3,li} = (s_1, s_2, c)$ 로 설정하는 과정을 통해 생성되는,

전자투표 방법.

청구항 12

제11항에 있어서,

상기 암호화된 증명표를 공개하는 단계 이후에,

상기 모든 유권자들의 제2 증명 값과 제3 증명 값의 유효성을 검증하는 단계를 더 포함하고,

상기 제2 증명 값과 상기 제3 증명 값의 유효성을 검증하는 단계는,

$c = H(l \parallel g \parallel X_{l,i} \parallel U_{l,i} \parallel g^{s_1} X_{l,i}^{d_1} \parallel Y_{l,i}^{s_1} U_{l,i}^{d_1} \parallel g^{s_2} X_{l,i}^{d_2} \parallel Y_{l,i}^{s_2} (U_{l,i}/g)^{d_2})$ 및

$c = H(l \parallel g \parallel U_{l,i} \parallel V_{l,i} \parallel Y_{l,i}^{s_1} g^{s_2} U_{l,i}^c \parallel Z_{l,i}^{s_1} g^{s_2} V_{l,i}^c)$ 의 성립 여부를 판단하는,
전자투표 방법.

청구항 13

제12항에 있어서,

상기 제2 증명 값과 상기 제3 증명 값의 유효성을 검증하는 단계는,

$$\prod_{i=1}^k V_{l,i} = \prod_{i=1}^k Z_{l,i}^{x_{l,i}} g^{v_{l,i}} = g^1$$

의 성립 여부를 더 판단하는,

전자투표 방법.

청구항 14

제13항에 있어서,

상기 찬성표의 개수를 계산하는 단계는,

$$\prod_{j=1}^n U_{j,i} = g^{\sum_{j=1}^n v_{j,i}}$$

모든 $i \in [k]$ 에 대해 를 계산하는 단계, 및

$$g^{\gamma_i} = g^{\sum_{j=1}^n v_{j,i}}$$

모든 $i \in [k]$ 에 대해 를 만족하는 γ_i 를 계산하는 단계를 포함하는,

전자투표 방법.

발명의 설명

기술 분야

[0001] 본 발명은 탈중앙 전자투표 시스템에 관한 것으로, 보다 구체적으로 투표에 참여하는 모든 유권자는 별도의 신뢰기관 없이 스스로 투표 및 개표를 수행할 수 있으며 모든 유권자가 정당하게 투표를 수행하여 개표의 결과가 올바른 결과임을 누구나 검증할 수 있는 탈중앙 전자투표 시스템에 관한 것이다.

배경 기술

[0002] 익명투표는 민주주의 사회에서 조직 구성원의 의견을 수렴하기 위한 필수적인 수단이다. 인터넷의 발달과 함께 암호기술을 사용하여 안전성과 효율성을 보장하는 다양한 전자 투표 시스템이 제안되었으며 이를 통해 기존의 투표 용지를 사용하는 방식의 익명투표보다 비용과 시간 측면에서 많은 개선이 이루어졌다. 하지만 초기의 많은 전자투표 시스템은 전통적으로 암호화된 표를 취합하여 이로부터 개표를 수행하는 별도의 신뢰기관을 두어 동작하는 방식을 채택해왔다. 이러한 투표방식의 치명적인 단점은 별도 기관의 존재이며 모든 유권자는 해당 기관을 신뢰하여야 한다는 점으로, 이러한 단점을 보완하기 위해 임계치 기법(Threshold cryptography)을 이용하여 하나의 신뢰기관에 대한 신뢰를 분산하여 다수의 기관을 두어 운용할 수 있지만 이러한 투표 시스템 또한 다수의 기관이 공모하지 않을 것이라는 신뢰가 반드시 필요하다.

[0003] 이러한 신뢰 문제를 해결하기 위해 자가 개표(Self tallying)를 지원하는 투표 시스템이 개발되었다. 자가 개표를 지원하는 투표 시스템은 모든 유권자들로부터 공개된 암호화된 표로부터 누구나 개표를 수행할 수 있게 함으로써 개표를 위한 별도의 신뢰기관을 필요로 하지 않는다. 자가 개표를 지원하는 투표 시스템을 실현하기 위한 핵심 기술로는 암호화 후 소거법(Encrypt-then-cancel rule)과 영지식 증명(Zero-knowledge proof) 기술이 있으며 유권자는 암호화 후 소거법을 이용하여 본인의 표를 암호화함과 동시에 다른 유권자들로부터 공개된 암호화된 표로부터 암호화에 사용된 난수들을 소거하여 개표를 수행할 수 있다. 또한 모든 유권자는 본인의 표를 노출시키지 않으면서 정당한 표를 암호화하였다는 사실을 증명하기 위한 수단으로 영지식 증명 기술을 사용한다.

[0004] 실생활에서 운용되는 대부분의 투표 시스템은 후보의 수가 다수인 경우가 일반적이기 때문에 후보의 수를 확장하는 데에 드는 비용을 최소화하여 효율성을 높이는 것이 중요하다. 더불어 블록체인 기술의 발전과 함께 암호

화폐 등 다양한 분야에서 탈중앙 시스템의 중요성이 대두되고 있고, 이에 따라 자가 개표를 지원하는 전자투표 시스템 또한 많은 연구가 이루어지고 있다. 하지만 현재까지 알려진 자가 개표를 지원하는 전자투표 시스템은 후보가 다수인 환경에서 개표에 필요한 연산량이 후보의 수에 따라 기하급수적으로 증가한다는 한계점으로 인해 찬반투표와 같이 극히 제한적인 상황에서만 사용할 수 있다. 따라서 자가 개표를 지원하는 탈중앙 투표시스템에서 개표의 효율성을 높이는 것은 반드시 개선되어야 할 중요한 과제이다.

선행기술문헌

특허문헌

- [0005] (특허문헌 0001) 대한민국 공개특허 제2020-0111416호 (2020.09.29. 공개)
(특허문헌 0002) 대한민국 공개특허 제2012-0028157호 (2012.03.22. 공개)

비특허문헌

- [0006] (비특허문헌 0001) F. Hao and P. Zieli'nski, "2-round anonymous veto protocol," in International Workshop on Security Protocols. Springer, 2006, pp. 202-211.
(비특허문헌 0002) F. Hao, P. Y. Ryan, and P. Zieli'nski, "voting by two-round public discussion," IET Information Security, vol. 4, no. 2, pp. 62-67, 2010.

발명의 내용

해결하려는 과제

- [0007] 본 발명이 이루고자 하는 기술적인 과제는 후보가 다수인 환경에서 효율적으로 동작하는 탈중앙 전자투표 시스템을 제공하는 것이다.

과제의 해결 수단

- [0008] 본 발명의 일 실시예에 따른, 후보가 다수인 환경에서 효율적으로 동작하는 탈중앙 전자투표 방법은 유권자의 단말에 의해 수행되는 전자투표 방법으로, 소수(p)에 대한 군(G)와 상기 군(G)의 생성자(g)에 대한 (G, g) 에 대하여 합의하는 단계, 비밀 투표키와 공개 투표키를 생성하고 상기 공개 투표키를 공개하는 단계, 복수의 후보들에 대한 암호화된 행사표와 암호화된 증명표를 생성하는 단계, 상기 암호화된 행사표를 공개하는 단계, 상기 암호화된 증명표를 공개하는 단계, 및 모든 유권자들의 행사표에 기초하여 복수의 후보들 각각에 대한 찬성표의 개수를 계산하는 단계를 포함한다.

발명의 효과

- [0009] 본 발명의 실시예에 따른 탈중앙 전자투표 시스템 및 방법에 의할 경우, 후보가 다수인 환경에서도 효율적으로 동작하는 탈중앙 전자투표 기법을 제공할 수 있다.
[0010] 또한, 기존 기법에 비해, 개표를 위한 연산량을 획기적으로 감소시킬 수 있는 효과가 있다.

도면의 간단한 설명

- [0011] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
도 1은 본 발명의 일 실시예에 따른 전자투표 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0012] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

- [0013] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.
- [0014] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.
- [0015] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.
- [0016] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0017] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0018] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [0019] 우선, 본 발명을 위한 기본 지식으로써, 암호화 후 소거법(Encrypt-then-cancel rule)과 DDH(Decision Diffie-Hellman) 가정에 대해 설명한다.
- [0020] 암호화 후 소거법(Encrypt-then-cancel rule)
- [0021] 암호화 후 소거법에 대한 아이디어는 익명으로 거부권(veto)을 행사할 수 있는 시스템(anonymous veto protocol) 설계를 위해 F. Hao 등의 연구(F. Hao and P. Zieli'nski, "2-round anonymous veto protocol," in International Workshop on Security Protocols. Springer, 2006, pp. 202-211.)에서 처음 소개되었다.
- [0022] F. Hao 등의 연구에서 소개된 시스템에서는 모든 참여자가 거부권을 행사하지 않았는지, 아니면 한명의 참여자라도 거부권을 행사하였는지에 대해 그 결과가 0 또는 1이었던 반면, F. Hao 등의 연구(F. Hao, P. Y. Ryan, and P. Zieli'nski, "voting by two-round public discussion," IET Information Security, vol. 4, no. 2, pp. 62-67, 2010.)에서는 찬반투표(찬성표와 반대표가 각각 몇표인지) 뿐만 아니라 후보가 다수인 환경에서 한명의 후보를 선출하는 일반적인 투표시스템에서 사용될 수 있게 되었다.
- [0023] 암호화 후 소거법은 n 명의 참여자와 각각의 사용자가 숨기고자 하는 데이터에 대해 아래와 같은 순서로 진행된다.
- [0024] 1. 모든 참여자에 대해 순서를 할당한 리스트($P_1, P_2, \dots, P_n$)을 정하고, 모든 유권자는 DDH 가정을 만족하는 큰 소수 p 에 대한 군 G 와 해당 군의 생성자 g 에 대한 (G, g) 에 합의한다.
- [0025] 2. 각각의 참여자 P_i 는 비밀키 $x_i \in \mathbb{Z}_p$ 를 추출한다.

[0026] 3. P_i 는 x_i 를 이용하여 공개키 $X_i = g^{x_i}$ 를 계산하여 공개한다.

[0027] 4. P_i 는 본인을 제외한 모든 참여자가 공개한 공개키를 이용하여 $Y_i = g^{y_i}$ 를 아래와 같이 계산한다.

[0028]

$$Y_i = \begin{cases} 1 / \prod_{j=2}^n X_j & (i=1), \\ \prod_{j=1}^{i-1} X_j / \prod_{j=i+1}^n X_j & (2 \leq i \leq n-1), \\ \prod_{j=1}^{n-1} X_j & (i=n). \end{cases}$$

[0029] 5. P_i 는 숨기고자 하는 데이터 d_i 를 본인의 비밀키 x_i 와 위에서 계산한 Y_i 를 이용하여 $U_i = (Y_i)^{x_i} g^{d_i}$ 암호화하여 공개한다.

[0030] 6. 모든 참여자가 공개한 암호화된 데이터 $U_i = (Y_i)^{x_i} g^{d_i}$ 를 이용하여 $\prod_{i=1}^n U_i$ 를 계산한다. 이때, 표 1(n=5인 경우, $x_i x_j$ 의 부호)에 의해 $\sum_{i=1}^n x_i y_i = \sum_{i=1}^n x_i \left(\sum_{j=1}^{i-1} x_j - \sum_{j=i+1}^n x_j \right)$ 는 0으로 모두 소거되어 $\prod_{i=1}^n U_i = \prod_{i=1}^n g^{x_i y_i} g^{d_i} = g^{\sum_{i=1}^n d_i}$ 이 성립한다.

[0031] 7. P_i 는 $g^\gamma = g^{\sum_{i=1}^n d_i}$ 를 만족하는 γ 를 전수조사를 통해 계산하여 모든 참여자의 데이터들의 합 $(d_1 + d_2 + \dots + d_n)$ 을 얻을 수 있다.

[0032] DDH(Decision Diffie-Hellman) 가정

[0033] 소수 p 에 대해 위수가 p 인 군 G , G 의 생성자 g , 그리고 $a, b \in \mathbb{Z}_p$ 에 대해 튜플 (g, g^a, g^b, T) 이 주어졌을 때, $T = g^{ab}$ 인지 아닌지 결정하는 문제를 DDH 문제라고 한다.

[0034] 다항시간 공격자(probabilistic-polynomial-time adversary)가 DDH 문제를 해결할 확률이 극히 희박하다면 DDH 가정이 성립한다고 정의한다.

[0035] 이하에서는, 본 명세서에서 사용되는 표기에 대해 설명한다.

[0036] - $a \parallel b$: 문자열 a 와 b 의 연결 (예를 들어, $a=110$ 이고 $b=101$ 이면 $a \parallel b$ 는 110101)

[0037] - $[k]$: 정수집합 $\{1, 2, \dots, k\}$

[0038] - $A \setminus B$: 두 집합 A 와 B 의 차집합 (예를 들어, $A=\{1, 2, 3, 4\}$ 이고 $B=\{2, 4\}$ 이면 $A \setminus B = \{1, 3\}$)

[0039] - $\mathbb{Z}_p$: 정수집합 $\{0, 1, 2, \dots, p-1\}$

[0040] - $H: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$: 암호학적으로 안전한 해시 함수. 임의의 문자열을 입력받아 $c \in \mathbb{Z}_p^*$ 를 출력하는 것으로 가정

[0041] - n : 전체 유권자의 수

[0042] - k : 전체 후보의 수

[0043] - P_i : i 번째 유권자

- [0044] - C_i : i 번째 후보
- [0045] - $v_{i,j}$: P_i 가 C_j 에게 행사하는 표로, 찬성일 경우 1, 반대일 경우 0으로 설정하여 $v_{i,j} \in \{0, 1\}$ 을 만족함
- [0046] 탈중앙 전자투표 시스템을 구성하는 객체는 P(유권자)와 C(후보)이다. 즉, 탈중앙 전자투표 시스템은 각각이 복수의 유권자들 각각에 대응되는 복수의 단말들로 구성될 수 있다. 상기 복수의 단말들 중 어느 하나는 소정의 유무선 통신망을 통하여 상기 복수의 단말들 중 다른 하나와 통신할 수 있다. 또한, 상기 복수의 단말들 각각은 스마트폰(smart phone), 모바일폰(mobile phone), PC(Personal Computer), 태블릿 PC, HMD(Head Mounted Device), 스마트 워치(smart watch), 스마트 안경(smart glasses), 노트북 등과 같이 적어도 프로세서(processor) 및/또는 메모리(memory)를 포함하는 컴퓨팅 장치를 의미할 수 있다. 따라서, 컴퓨팅 장치는 전자투표를 위한 단말, 전자투표 장치 등으로 명명될 수 있다.
- [0047] 탈중앙 전자투표 방법의 전체 프로토콜은 셋업(Setup), 라운드 1(Round 1), 라운드 2(Round 2), 및 자가 개표(Self-Tallying) 단계로 구성되며 각 알고리즘 및 프로토콜에 대한 설명은 아래와 같다. 또한, 본 발명의 일 실시예에 따른 전자투표 방법의 흐름도는 도 1에 도시되어 있다. 탈중앙 전자투표 방법을 이루는 단계들 중 적어도 일부는 컴퓨팅 장치의 프로세서의 동작으로 이해될 수도 있다.
- [0048] 셋업(Setup).
- [0049] n (n 은 2 이상의 자연수)명의 유권자와 k (k 은 2 이상의 자연수)명의 후보에 대해 각 유권자와 후보의 순서를 할당한 리스트 $(P_1, P_2, \dots, P_n)$ 와 $(C_1, C_2, \dots, C_k)$ 를 정하고, 모든 유권자(유권자의 단말을 의미할 수 있음)는 DDH 가정을 만족하는 큰 소수 p 에 대한 군 G 와 해당 군의 생성자 g 에 대한 (G, g) 에 대해 합의한다. 즉, 모든 유권자는 (G, g) 에 합의한 것으로 가정할 수 있다.
- [0050] 라운드 1(Round 1).
- [0051] 1. 각각의 유권자(유권자의 단말을 의미할 수 있음) P_i 은 모든 $i \in [k]$ 에 대한 k 개의 비밀 투표키(private voting keys) $x_{l,i} \in \mathbb{Z}_p$ 를 추출(선택이나 생성하는 것으로 이해될 수도 있음)한다.
- [0052] 2. P_i 은 모든 $i \in [k]$ 에 대해 $x_{l,i}$ 를 이용하여 공개 투표키(public voting keys) $X_{l,i} = g^{x_{l,i}}$ 를 계산한다.
- [0053] 3. P_i 은 모든 $i \in [k]$ 에 대해 자신의 비밀 투표키 $x_{l,i} \in \mathbb{Z}_p$ 를 알고 있다는 사실을 비대화형 영지식(non-interactive zero-knowledge, NIZK) 프로토콜을 이용하여 증명한다. 영지식 프로토콜의 증명 값은 $\pi_{1,i} = \text{NIZK} \{x_{l,i} : X_{l,i} = g^{x_{l,i}}\}$ 로 나타낼 수 있으며 아래 과정을 통해 생성된다. 이와 관련하여, 표 1은 n 명의 유권자에 의해 공개된 공개 투표키를 나타낸다.
- [0054] 3.1. 임의의 $r \in \mathbb{Z}_p$ 를 선택한다.
- [0055] 3.2. $a = g^r$ 를 계산한다.
- [0056] 3.3. 암호학적 해시 함수 H 를 이용하여 $c = H(i \parallel g \parallel X_{l,i} \parallel a)$ 를 계산한다.
- [0057] 3.4. $s = r - x_{l,i}c$ 를 계산한다.
- [0058] 3.5. 증명 값을 $\pi_{1,i} = (s, c)$ 로 설정한다.
- [0059] 4. P_i 은 모든 $i \in [k]$ 에 대해 $X_{l,i}$ 와 $\pi_{1,i}$ 를 공개한다.
- [0060] 5. P_i 은 본인을 제외한 모든 유권자가 모든 후보, 즉 $j \in [n] \forall$ 와 $i \in [k]$ 을 만족하는 모든 (j, i) 에 대해 $\pi_{1,i}$ 가 유효한지 검증하기 위해 $c = H(i \parallel g \parallel X_{j,i} \parallel g^s X_{j,i}^c)$ 이 성립하는지 확인한다. 성립하면 다음으로 넘어가고, 하나라도 성립하지 않으면 프로토콜 진행을 중단하고 0을 출력한다.

6. P_l 은 본인을 제외한 모든 유권자가 공개한 공개 투표키를 이용하여 $Y_{l,i}$ 와 $Z_{l,i}$ 를 아래와 같이 계산한다.

$$Y_{l,i} = \begin{cases} 1 / \prod_{j=2}^n X_{j,i} & (l=1), \\ \prod_{j=1}^{l-1} X_{j,i} / \prod_{j=l+1}^n X_{j,i} & (2 \leq l \leq n-1), \\ \prod_{j=1}^{n-1} X_{j,i} & (l=n). \end{cases}$$

$$Z_{l,i} = \begin{cases} 1 / \prod_{j=2}^k X_{l,j} & (i=1), \\ \prod_{j=1}^{i-1} X_{l,j} / \prod_{j=i+1}^k X_{l,j} & (2 \leq i \leq k-1), \\ \prod_{j=1}^{k-1} X_{l,j} & (i=k). \end{cases}$$

[표 1]

P_1	$g^{x_{1,1}}$	$g^{x_{1,2}}$	$\dots$	$g^{x_{1,k}}$
P_2	$g^{x_{2,1}}$	$g^{x_{2,2}}$	$\dots$	$g^{x_{2,k}}$
$\vdots$		$\vdots$		
P_n	$g^{x_{n,1}}$	$g^{x_{n,2}}$	$\dots$	$g^{x_{n,k}}$

* i -th voter: P_i

* Public voting key of P_i for j -th candidate: $g^{x_{i,j}}$

라운드 2(Round 2).

1. 각각의 유권자 P_l 은 모든 $i \in [k]$ 에 대해 $v_{l,i}$ (행사표로 명명될 수 있음) 중 하나만을 찬성표(이 경우, $v_{l,i}=1$)로 설정하고, 다른 모든 표는 반대표(이 경우, $v_{l,i}=0$)로 설정하여 본인의 비밀 투표키 $x_{l,i}$ 와 위에서 계산한 $Y_{l,i}$ 와 $Z_{l,i}$ 를 이용하여 $U_{l,i} = Y_{l,i}^{x_{l,i}} g^{v_{l,i}}$ ((암호화된) 행생표로 명명될 수 있음)와 $V_{l,i} = Z_{l,i}^{x_{l,i}} g^{v_{l,i}}$ ((암호화된) 증명표로 명명될 수 있음)을 계산한다.

2. P_l 은 모든 $i \in [k]$ 에 대해 $U_{l,i}$ 를 계산하는 데에 사용한 $v_{l,i}$ 가 0 또는 1이라는 사실을 비대화식 영지식 증명 프로토콜을 이용하여 증명한다. 영지식 프로토콜의 증명 값은 $\pi_{2,li} = NIZK\{(x_{l,i}, v_{l,i}) : X_{l,i} = g^{x_{l,i}} \wedge U_{l,i} = (Y_{l,i})^{x_{l,i}} g^{v_{l,i}} \wedge v_{l,i} \in \{0,1\}\}$ 로 나타낼 수 있으며 아래 과정을 통해 생성된다.

2.1. $v_{l,i}=1$ 일 경우 아래 2.1.1.~2.1.5. 과정을 따르고, 그렇지 않을 경우 2.2.로 넘어간다.

2.1.1. 임의의 $r, s_1, d_1 \in \mathbb{Z}_p$ 를 선택한다.

2.1.2. $a_1 = g^{s_1} X_{l,i}^{d_1}$ 과 $b_1 = Y_{l,i}^{s_1} U_{l,i}^{d_1}$ 을 계산한다.

2.1.3. $a_2 = g^r$ 과 $b_2 = Y_{l,i}^r$ 을 계산한다.

2.1.4. 암호학적 해시 함수 H 를 이용하여 $c = H(l \parallel g \parallel X_{l,i} \parallel U_{l,i} \parallel a_1 \parallel b_1 \parallel a_2 \parallel b_2)$ 를 계산한다.

2.1.5. $d_2 = c - d_1$ 와 $s_2 = r - x_{l,i} d_2$ 을 계산한다.

- [0075] 2.2. $v_{l,i}=0$ 일 경우 아래 2.2.1.~2.2.6. 과정을 따른다.
- [0076] 2.2.1. 임의의 $r, s_2, d_2 \in \mathbb{Z}_p$ 를 선택한다.
- [0077] 2.2.2. $a_1 = g^r$ 과 $b_1 = Y_{l,i}^r$ 을 계산한다.
- [0078] 2.2.3. $a_2 = g^{s_2} X_{l,i}^{d_2}$ 과 $b_2 = Y_{l,i}^{s_2} (U_{l,i}/g)^{d_2}$ 을 계산한다.
- [0079] 2.2.4. 암호학적 해시 함수 H를 이용하여 $c = H(l \parallel g \parallel X_{l,i} \parallel U_{l,i} \parallel a_1 \parallel b_1 \parallel a_2 \parallel b_2)$ 를 계산한다.
- [0080] 2.2.5. $d_1 = c - d_2$ 와 $s_1 = r - x_{l,i} d_1$ 을 계산한다.
- [0081] 2.3. 증명 값을 $\pi_{2,li} = (s_1, s_2, d_1, d_2)$ 로 설정한다.
- [0082] 3. P_l 은 모든 $i \in [k]$ 에 대해 $U_{l,i}$ 와 $\pi_{2,li}$ 를 공개한다.
- [0083] 4. P_l 은 모든 $i \in [k]$ 에 대해 $U_{l,i}$ 와 $V_{l,i}$ 를 계산하는 데에 동일한 $x_{l,i}$ 와 $v_{l,i}$ 를 사용하였다는 사실을 비대화식 영 지식 증명 프로토콜을 이용하여 증명한다. 영지식 증명 프로토콜의 증명 값은 $\pi_{3,li} = NIZK\{(x_{l,i}, v_{l,i}) : U_{l,i} = (Y_{l,i})^{x_{l,i}} g^{v_{l,i}} \wedge V_{l,i} = (Z_{l,i})^{x_{l,i}} g^{v_{l,i}}\}$ 로 나타낼 수 있으며 아래 과정을 통해 생성된다.
- [0084] 4.1. 임의의 $r_1, r_2 \in \mathbb{Z}_p$ 를 선택한다.
- [0085] 4.2. $a = Y^{r_1} g^{r_2}$ 와 $b = Z^{r_1} g^{r_2}$ 를 계산한다.
- [0086] 4.3. 암호학적 해시 함수 H를 이용하여 $c = H(l \parallel g \parallel U_{l,i} \parallel V_{l,i} \parallel a \parallel b)$ 를 계산한다.
- [0087] 4.4. 증명 값을 $\pi_{3,li} = (s_1, s_2, c)$ 로 설정한다.
- [0088] 5. P_l 은 모든 $i \in [k]$ 에 대해 $V_{l,i}$ 와 $\pi_{3,li}$ 를 공개한다.
- [0089] 6. P_l 은 본인을 제외한 모든 유권자가 모든 후보, 즉 $j \in [n] \setminus i$ 와 $i \in [k]$ 을 만족하는 모든 (j, i) 에 대해 $\pi_{2,ji}$ 와 $\pi_{3,ji}$ 가 유효한지 검증하기 위해 아래 6.1.과 6.2.가 성립하는지 확인한다. 모두 성립하면 다음으로 넘어가고, 하나라도 성립하지 않으면 중단하고 0을 출력한다.
- [0090] 6.1. $c = H(l \parallel g \parallel X_{l,i} \parallel U_{l,i} \parallel g^{s_1} X_{l,i}^{d_1} \parallel Y_{l,i}^{s_1} U_{l,i}^{d_1} \parallel g^{s_2} X_{l,i}^{d_2} \parallel Y_{l,i}^{s_2} (U_{l,i}/g)^{d_2})$
- [0091] 6.2. $c = H(l \parallel g \parallel U_{l,i} \parallel V_{l,i} \parallel Y_{l,i}^{s_1} g^{s_2} U_{l,i}^c \parallel Z_{l,i}^{s_1} g^{s_2} V_{l,i}^c)$
- [0092] 7. P_l 은 본인을 제외한 모든 유권자, 즉 모든 $j \in [n] \setminus i$ 에 대해 $\prod_{i=1}^k V_{l,i} = \prod_{i=1}^k Z_{l,i}^{x_{l,i}} g^{v_{l,i}} = g^1$ 가 성립하는지 확인한다. 모두 성립하면 다음으로 넘어가고, 하나라도 성립하지 않으면 중단하고 0을 출력한다.
- [0093] 상술한 바와 같이, $\pi_{2,ji}$ 와 $\pi_{3,ji}$ 를 검증하고 식 $\prod_{i=1}^k V_{l,i} = \prod_{i=1}^k Z_{l,i}^{x_{l,i}} g^{v_{l,i}} = g^1$ 의 성립 여부를 체크함으로써, 일인 일투표(one-man-one-vote rule)를 검증할 수 있다.
- [0094] 자가 개표(Self-Tallying).

- [0095] 1. 각각의 유권자 P_i 은 모든 $i \in [k]$ 에 대해 $\prod_{j=1}^n U_{j,i} = g^{\sum_{j=1}^n v_{j,i}}$ 를 계산한다.
- [0096] 2. P_i 은 모든 $i \in [k]$ 에 대해 $g^{\gamma_i} = g^{\sum_{j=1}^n v_{j,i}}$ 를 만족하는 γ_i 를 전수조사를 통해 계산한다. 다시 말하면, 이산 로그 문제(discrete logarithm problem)를 풀이함으로써 γ_i 를 계산할 수 있다. 여기서, γ_i 는 i 번째 후보에 대한 찬성표의 개수를 의미할 수 있다.
- [0097] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 컨트롤러, ALU(Arithmetic Logic Unit), 디지털 신호 프로세서(Digital Signal Processor), 마이크로컴퓨터, FPA(Field Programmable array), PLU(Programmable Logic Unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(Operation System, OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(Processing Element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.
- [0098] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(Signal Wave)에 영구적으로, 또는 일시적으로 구체화(Embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0099] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-optical Media), 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0100] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

도면1

