

UNIVERSITATEA BABEȘ-BOLYAI
CLUJ-NAPOCA
FACULTATEA DE MATEMATICĂ ȘI
INFORMATICĂ
SPECIALIZAREA
MATEMATICĂ-INFORMATICĂ

LUCRARE DE LICENȚĂ

Sistem de vot electronic anonim
bazat pe tehnici criptografice

Conducător științific
Conf. Univ. Dr. BUFNEA Darius

Absolvent
Mazilu Paul-Constantin

ABSTRACT

The digital transformation of electoral systems has led to increased interest in secure and verifiable electronic voting solutions. This thesis presents the design and implementation of an electronic voting system that prioritizes usability, integrity, and voter privacy, while exploring cryptographic techniques to enhance confidentiality.

The paper begins with a theoretical foundation covering core principles of electronic voting, including anonymity, asymmetric cryptography (specifically RSA), and blind signature schemes. A comparative analysis of existing systems—such as Helios, REVS, and EVOX—is included to identify best practices and common vulnerabilities in current architectures.

Building on these concepts, the thesis proposes and implements a custom voting system developed with a modern web-based architecture. The backend is implemented using Spring Boot and PostgreSQL, with support for real-time result updates via WebSockets. The system supports multiple election types, encrypted vote storage, and anonymous ballot submission using RSA public-key encryption. Although the theoretical model includes support for blind signatures and full unlinkability, the current implementation focuses on vote confidentiality at storage and transmission level, without fully integrating cryptographic credential verification or a separate anonymizing network.

Votes are encrypted upon submission and stored independently from user identity, with authentication handled securely before ballot issuance. Additional features such as institutional and public elections, human validation of voters, voter profile management, and real-time analytics are included to demonstrate system scalability and adaptability.

The primary contribution of this work is the development of a practical, extensible platform that addresses key challenges in secure online voting. While not yet suitable for high-stakes national elections, the system provides a strong foundation for future research and development in verifiable and privacy-preserving digital voting.

Cuprins

1	Introducere	1
1.1	Contextul general al votului electronic	1
1.2	Motivația alegerii temei	1
1.3	Obiectivele cercetării	2
1.4	Metodologia cercetării	2
2	Fundamente teoretice și istorice ale votului electronic	3
2.1	Evoluția votului: de la fizic la electronic	3
2.2	Clasificarea sistemelor de vot electronic	3
2.3	Beneficii și riscuri ale votului electronic	4
2.4	Inițiative internaționale notabile	4
2.5	Cerințe de securitate în e-voting	4
3	Criptografie aplicată în votul electronic	6
3.1	Noțiuni fundamentale	6
3.2	Algoritmul RSA	7
3.3	Semnături digitale și verificare	8
3.4	Semnături oarbe (Blind Signatures)	9
3.4.1	Exemplu ilustrativ	10
3.5	Standardele criptografice aplicate	10
3.5.1	Standardele respectate în sistemul propus:	11
3.6	Comparație între tehnici criptografice utilizate în votul electronic	11
3.6.1	Criptare ElGamal	12
3.6.2	Mix-net-uri	12
3.6.3	Compararea abordărilor	13
4	Puterea de Vot – Fundamente Matematice, Statistice și Indici Cantitativi	14
4.1	Introducere	14
4.2	Modelarea Probabilistică a Puterii de Vot	14
4.3	Vot Ponderat și Paradoxuri	15
4.4	Indici Cantitativi: Banzhaf și Shapley-Shubik	15

4.5	Aproximații și Teoreme	19
4.6	Simulări și Algoritmi Practici	20
4.7	Modelarea Dependentei Voturilor și Preferințelor Latente	20
4.7.1	Modelare Discretă a Dependentei Voturilor	21
4.7.2	Modelare Continuă a Preferințelor Latente	21
4.8	Modele Alternative: Corelare și Rețele	22
4.9	Aplicabilitate în Sisteme Electronice de Vot	23
5	Analiza comparativă	24
5.1	Criterii de evaluare	24
5.2	Sistemul Helios	24
5.3	Sistemul Estonia i-Voting	25
5.4	Sistemul REVS	25
6	Arhitectura sistemului de vot anonim	27
6.1	Prezentare generală	27
6.2	Arhitectura pe straturi	27
6.3	Modelul bazei de date	28
6.3.1	Entități principale	29
6.3.2	Principii de proiectare	29
6.4	Modelul domeniului și diagrama de clase	31
6.4.1	Principii de proiectare	31
6.4.2	Diagramă de clase	32
6.4.3	Fluxul de vot anonim	33
7	Implementarea sistemului de vot electronic	34
7.1	Tehnologiile utilizate	34
7.2	Funcționalități implementate	35
7.2.1	Înregistrare și autentificare	35
7.2.2	Verificarea identității	36
7.2.3	Gestionarea alegerilor	37
7.2.4	Mecanismul de votare anonimă	39
7.2.5	Numărarea voturilor în timp real și finală	40
7.2.6	Administrare	42
7.3	Criptarea în sistemul de vot electronic	42
7.3.1	Structura modulelor criptografice	42
7.3.2	Etapele procesului criptografic	43
7.3.3	Separarea identității de conținutul votului	44
8	Măsuri de securitate în sistemul de vot	45

8.1	Modelul de securitate aplicat	45
8.2	Izolarea identității alegătorului	45
8.3	Prevenirea votului multiplu	46
8.4	Criptarea votului și integritatea datelor	46
8.5	Controlul accesului și validarea datelor	46
8.6	Canalul de comunicare	46
9	Importanța sociologică a votului într-o societate democratică	48
9.1	Votul ca fundament al democrației	48
9.2	Dimensiunea socială și identitară a votului	48
9.3	Consecințele absenteismului și ale neîncrederii	48
9.4	Capitalul social și implicarea civică	49
9.5	Considerații legale și etice	49
9.6	Rolul votului electronic în extinderea participării	49
9.7	Votul și responsabilitatea civică	50
9.8	Acceptabilitatea votului electronic în România	50
9.8.1	Studiile internaționale și europene	50
9.8.2	Atitudinea alegătorilor români	50
10	Concluzii	51

Capitolul 1

Introducere

1.1 Contextul general al votului electronic

Digitalizarea accelerată a serviciilor publice și extinderea infrastructurilor informatice au creat premisele unei transformări profunde a proceselor electorale. În acest peisaj tehnologic, votul electronic s-a conturat ca o alternativă viabilă la metodele tradiționale de vot, fiind testat sau implementat în diverse forme în țări precum Estonia, Elveția, Canada și SUA. Principalele avantaje asociate includ: creșterea accesibilității, eficiența administrativă și integrarea tehnologiilor avansate de criptare pentru protejarea datelor sensibile.

Totuși, odată cu oportunitățile apar și provocări majore. Orice sistem de vot online trebuie să respecte o serie de cerințe fundamentale, precum: securitatea, confidențialitatea, integritatea, verificabilitatea și anonimatul. Orice compromis în aceste direcții poate afecta direct încrederea cetățenilor și legitimitatea alegerilor.

1.2 Motivația alegerii temei

Alegerea temei este motivată de nevoia reală de a proiecta și implementa un sistem de vot electronic care să ofere nu doar funcționalitate, ci și garanții solide de securitate și anonimat. Majoritatea soluțiilor existente nu oferă separare completă între identitatea alegătorului și opțiunea sa de vot, ceea ce poate duce la vulnerabilități grave din punct de vedere etic și legal.

Dincolo de dimensiunea practică, tema permite explorarea unor concepte avansate de criptografie aplicată, cu accent pe semnături oarbe (blind signatures) și criptare asimetrică RSA. Aceasta oferă un cadru ideal pentru a integra cunoștințe teoretice cu implementare concretă, în contextul unui domeniu cu impact social major.

1.3 Obiectivele cercetării

Scopul principal al lucrării este dezvoltarea unei aplicații web care să permită votul electronic anonim, bazat pe semnături oarbe și criptografie RSA, fără posibilitatea corelării între alegător și vot. Obiectivele urmărite sunt:

- Investigarea cerințelor funcționale și de securitate ale unui sistem de vot electronic;
- Studierea metodelor criptografice care asigură confidențialitate și anonimat;
- Definirea unei arhitecturi modulare și sigure pentru aplicația propusă;
- Implementarea sistemului folosind tehnologii moderne (Spring Boot, PostgreSQL, WebSocket, RSA);
- Evaluarea limitărilor și identificarea unor direcții de extindere.

1.4 Metodologia cercetării

Abordarea este una mixtă, care combină cercetarea teoretică cu implementarea practică. Analiza bibliografică a fost folosită pentru fundamentarea criptografică și explorarea soluțiilor existente. Partea practică constă în proiectarea, codarea și testarea unei aplicații reale de vot electronic anonim, capabilă să gestioneze alegeri, să valideze alegători, să emită tokenuri și să proceseze voturi criptate.

Capitolul 2

Fundamente teoretice și istorice ale votului electronic

2.1 Evoluția votului: de la fizic la electronic

Procesul de votare a trecut prin numeroase transformări de-a lungul istoriei, de la exprimarea verbală a preferințelor până la buletinele de vot tipărite și sisteme digitale. Primele inițiative de automatizare au apărut încă din secolul XIX, odată cu brevetul lui Thomas Edison pentru o mașină de înregistrare a voturilor. Cu timpul, sistemele de vot au evoluat către variante bazate pe cartele perforate, urne electronice și, recent, platforme de vot la distanță prin internet.[Gri03]

Tranziția către votul electronic a fost determinată de dorința de eficientizare, reducerea erorilor umane, creșterea participării și scăderea costurilor electorale. Totuși, acest progres tehnologic a fost însoțit de provocări privind securitatea, transparența și încrederea publicului.[Riv06]

2.2 Clasificarea sistemelor de vot electronic

Sistemele de vot electronic pot fi clasificate în funcție de modul de utilizare și de gradul de control:

- **Vot electronic asistat (poll-site e-voting)** – realizat în secții dotate cu terminale electronice;
- **Vot prin internet (remote e-voting)** – permite exprimarea votului de la distanță, de obicei printr-un browser securizat[OSC13];
- **Vot prin SMS sau aplicații mobile** – folosit în experimente și voturi consultative;

- **Vot blockchain** – sistem emergent, cu accent pe transparență și imutabilitate.

Fiecare categorie implică niveluri diferite de securitate, auditabilitate și accesibilitate.

2.3 Beneficii și riscuri ale votului electronic

Printre avantajele majore se numără:

- Acces facil pentru persoane aflate în străinătate sau cu dizabilități;
- Numărare automată, rapidă și fără erori umane;
- Costuri reduse pe termen lung;
- Posibilitatea integrării de mecanisme criptografice pentru verificabilitate.

Pe de altă parte, riscurile includ:

- Lipsa transparenței pentru alegătorul obișnuit;
- Vulnerabilități la atacuri informatice sau manipulări;
- Riscul pierderii anonimității;
- Dificultăți în asigurarea coerciției nule și a autenticității.

2.4 Inițiative internaționale notabile

Estonia este considerată pionier în implementarea votului prin internet, oferind această posibilitate cetățenilor încă din 2005. Alte țări, precum Elveția, Norvegia sau Franța, au testat sau folosit sisteme similare în contexte limitate. De asemenea, organizații precum OSCE sau Consiliul Europei au emis recomandări și standarde pentru sistemele de e-voting.[SR21; Eur04]

Un exemplu notabil este sistemul Helios, o platformă open-source care oferă verificabilitate criptografică, însă nu garantează anonimitatea deplină a votului.

2.5 Cerințe de securitate în e-voting

Un sistem de vot electronic robust trebuie să satisfacă următoarele cerințe:

- **Eligibilitate** – doar alegătorii autorizați pot vota;
- **Unicitate** – fiecare alegător poate vota o singură dată;

- **Integritate** – voturile nu pot fi modificate sau șterse;
- **Confidențialitate** – alegerea votantului rămâne secretă;
- **Verificabilitate** – rezultatele pot fi verificate public;
- **Rezistență la coerciție** – votantul nu poate fi forțat să voteze într-un anumit fel;
- **Anonimitate completă** – votul nu trebuie să poată fi asociat cu identitatea alegătorului.

Aceste cerințe formează baza teoretică pentru proiectarea oricărui sistem modern de e-voting. [Gri03; Cha81; OSC13; Eur04]

Capitolul 3

Criptografie aplicată în votul electronic

3.1 Noțiuni fundamentale

Criptografia este o ramură a matematicii și informaticii care se ocupă cu studiul metodelor de transformare a informației în scopul protejării confidențialității, autenticității și integrității acesteia. De-a lungul istoriei, criptografia a fost folosită pentru a proteja comunicațiile diplomatice, militare sau comerciale, iar în prezent reprezintă un pilon fundamental al securității cibernetice.

Primele forme de criptografie datează din Antichitate — celebrul cifru Caesar fiind un exemplu timpuriu de criptare prin substituție. În Evul Mediu și Renaștere, criptografia a fost rafinată de matematicieni precum Al-Kindi sau Vigenère, dar abia în secolul XX aceasta s-a formalizat matematic.

În era modernă, criptografia s-a dezvoltat pe baze riguroase, utilizând concepte din teoria numerelor, algebra modulară și complexitatea computațională. În special, apariția criptografiei asimetrice în anii 1970 a marcat o revoluție în securitatea digitală, permițând schimbul de informații în siguranță între părți care nu se cunosc.

În contextul votului electronic, criptografia este indispensabilă. Ea oferă **Confidențialitate, Integritate, Autentificare și Anonimitate**.

Din punct de vedere tehnic, criptografia modernă se împarte în două mari categorii [Sta11; MOV96]:

- **Criptografia simetrică** – utilizează aceeași cheie pentru criptare și decriptare (e.g. Advanced Encryption Standard). Este rapidă și eficientă, dar necesită un canal securizat pentru distribuirea cheii.
- **Criptografia asimetrică** – folosește o pereche de chei: una publică pentru criptare și una privată pentru decriptare. Este potrivită în contexte fără partaj prealabil de chei, precum transmiterea voturilor într-un sistem electronic.

În cadrul sistemului nostru de vot, criptografia asimetrică joacă un rol central, în special prin utilizarea RSA atât pentru criptarea voturilor, cât și pentru semnături oarbe care permit autentificarea fără a compromite anonimitatea.

3.2 Algoritmul RSA

RSA (Rivest–Shamir–Adleman) este unul dintre cele mai cunoscute și utilizate algoritme criptografice asimetrice. A fost publicat pentru prima dată în anul 1977 de către cercetătorii Ron Rivest, Adi Shamir și Leonard Adleman de la MIT, fiind primul algoritm practic care permite atât criptare, cât și semnături digitale printr-o pereche de chei publică/privată.[RSA78]

Securitatea RSA se bazează pe dificultatea factorizării numerelor mari, problemă considerată computațional intractabilă pentru valori suficient de mari ale cheilor (2048 biți sau mai mult).

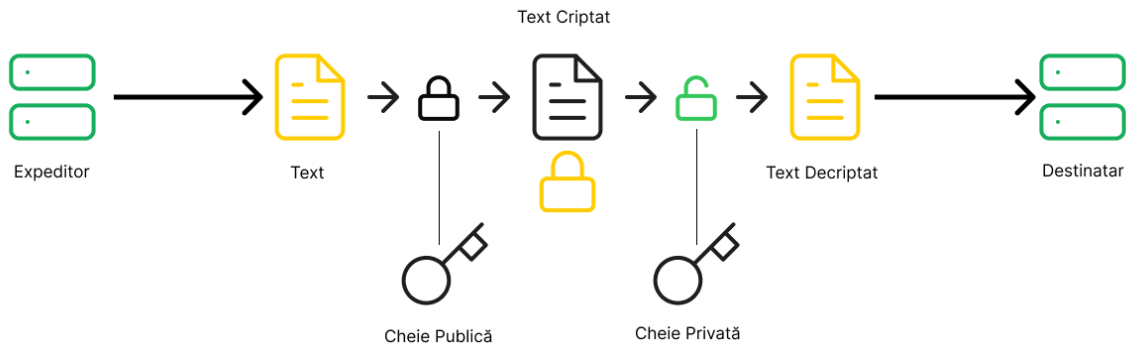


Figura 3.1: Funcționarea cifrului RSA

Algoritmul presupune următorii pași pentru generarea cheilor:

1. Alegerea a două numere prime mari: p și q .
2. Calcularea $n = p \cdot q$ și a funcției lui Euler: $\varphi(n) = (p - 1)(q - 1)$.
3. Alegerea unui exponent public e astfel încât $\gcd(e, \varphi(n)) = 1$ (valori comune sunt 3, 17 sau 65537).
4. Calcularea exponentului privat d ca invers modular: $d \equiv e^{-1} \pmod{\varphi(n)}$.

Criptarea unui mesaj m (numeric, $m < n$) se face conform specificațiilor din [MKJ16]:

$$c = m^e \pmod{n} \quad (3.1)$$

Decriptarea se face cu cheia privată:

$$m = c^d \mod n \quad (3.2)$$

RSA este un algoritm determinist în forma sa simplă, dar în practică se folosește întotdeauna împreună cu funcții de padding (e.g. Optimal Asymmetric Encryption Padding sau Probabilistic Signature Scheme) pentru a preveni atacuri.[MKJ16]

3.3 Semnături digitale și verificare

Semnătura digitală este un mecanism criptografic esențial pentru validarea autenticității și integrității unui mesaj. Conceptul de semnătură digitală a fost formalizat în anii 1970 și s-a dezvoltat semnificativ odată cu apariția algoritmilor asimetrice, în special RSA.[DH76]

În cazul RSA, semnarea presupune aplicarea cheii private d asupra unui mesaj m sau asupra unei amprente (hash) a acestuia. Semnătura rezultată conform [MKJ16; DH76] este:

$$s = m^d \mod n \quad (3.3)$$

Verificarea se face public, aplicând exponentul e :

$$m \stackrel{?}{=} s^e \mod n \quad (3.4)$$

În practică, semnătura nu se aplică direct pe mesajul brut, ci pe un rezumat criptografic al acestuia (de exemplu, SHA-256)[MKJ16]. Astfel, procesul real implică:

- calculul hash-ului mesajului:

$$h = \text{SHA-256}(m) \quad (3.5)$$

- semnarea hash-ului:

$$s = h^d \mod n; \quad (3.6)$$

- verificarea:

$$h \stackrel{?}{=} s^e \mod n \quad (3.7)$$

Acest mecanism este utilizat pe scară largă în protocoale de securitate (TLS, semnătura fișierelor PDF, GPG, etc.) și reprezintă un element important pentru sistemele de vot verificabile.

3.4 Semnături oarbe (Blind Signatures)

Conceptul de semnături oarbe a fost introdus de **David Chaum** în 1982, într-un articol fundamental care a pus bazele criptografiei anonime. Spre deosebire de semnăturile digitale clasice, semnăturile oarbe permit unei entități (ex. un alegător) să obțină o semnătură validă asupra unui mesaj fără ca semnatarul (ex. autoritatea electorală) să cunoască conținutul acelui mesaj.[Cha82]

Procesul se bazează pe mascarea (orbirea) mesajului original înainte de semnare. În cazul RSA, dacă un alegător vrea să obțină o semnătură pe un mesaj m , el va genera un factor aleator r și va calcula conform [MKJ16; RSA78]:

$$m' = m \cdot r^e \mod n \quad (3.8)$$

Semnătura asupra mesajului orbit este:

$$s' = (m')^d \mod n \quad (3.9)$$

După primirea semnăturii, alegătorul „dezorbește” semnătura:

$$s = s' \cdot r^{-1} \mod n \quad (3.10)$$

Rezultatul s este o semnătură validă pentru mesajul m , verificabilă ca orice semnătură RSA:

$$m = s^e \mod n \quad (3.11)$$

Avantajul esențial este că semnatarul nu are nicio informație despre m , deci nu poate corela semnătura cu identitatea solicitantului. Această proprietate este fundamentală pentru sistemele de vot electronic anonim și pentru aplicații precum e-cash, autentificare anonimă sau validare de tokenuri.[Gri03; SB23]

Sistemul propus urmărește respectarea unor proprietăți esențiale pentru securitatea și confidențialitatea votului electronic: **verificabilitatea**, care permite oricui să valideze faptul că un vot a fost corect exprimat; **anonimitatea**, ce asigură că identitatea alegătorului nu poate fi asociată cu votul său; și **unlinkability** (dezlegarea identității), care garantează că nu se poate realiza nicio corelare între un vot și un anumit credential de autentificare. Aceste cerințe sunt îndeplinite în implementare prin utilizarea semnăturilor oarbe pentru autorizarea anonimă a votantului, criptarea votului utilizând algoritmul RSA și proiectarea bazei de date astfel încât să nu existe nicio legătură între identitatea utilizatorului și votul salvat.

3.4.1 Exemplu ilustrativ

Presupunem:

$$p = 11, \quad q = 13 \Rightarrow n = 143, \quad \varphi(n) = 120, \quad e = 7, \quad d = 103 \quad (3.12)$$

Alegătorul vrea să voteze $m = 9$ cu factor de orbire $r = 5$:

$$m' = 9 \cdot 5^7 \mod 143 = 109, \quad s' = 109^{103} \mod 143, \quad s = s' \cdot r^{-1} \mod 143 \quad (3.13)$$

Această semnătură s este validă pentru m și verificabilă cu cheia publică.

3.5 Standardele criptografice aplicate

Pentru a construi un sistem de vot electronic robust și interoperabil, este esențială respectarea unor standarde criptografice recunoscute la nivel internațional. Acestea asigură nu doar siguranța matematică a algoritmilor utilizați, ci și compatibilitatea cu alte sisteme și bune practici în domeniul securității informației.[SB23; MKJ16; Nat19]

- **RFC 9474 – RSA Blind Signatures** Acest standard definește un protocol criptografic pentru semnături oarbe folosind RSA, astfel încât semnatarul (autoritatea) să nu cunoască mesajul semnat. Protocolul include metode pentru orbirea, semnarea și dezorbirea mesajului într-un mod sigur, precum și considerente despre atacuri posibile. Este un reper important pentru aplicații în care anonimitatea este esențială, cum este cazul votului electronic.
- **RFC 8017 (PKCS #1 v2.2)** Acesta este standardul principal care specifică algoritmul RSA, incluzând:
 - **RSAPSS-OAEP** – o schemă de criptare cu padding sigur, utilizată pentru criptarea voturilor;
 - **RSASSA-PSS** – schemă modernă de semnătură digitală, cu protecție împotriva atacurilor de tip replay și coliziuni;
 - **Formate standard** pentru generarea și reprezentarea cheilor.

PKCS #1 oferă un cadru formalizat, adoptat pe scară largă în sisteme care folosesc RSA.

- **NIST SP 800-56B (Rev. 2)** Publicat de National Institute of Standards and Technology (SUA), acest standard definește cerințele pentru generarea, validarea și gestionarea cheilor criptografice în sisteme bazate pe algoritmi asimetrici. Include:

- recomandări privind lungimea cheilor (2048+ biți pentru RSA),
- reguli pentru generarea perechilor unice de chei,
- separarea cheilor pentru semnare față de criptare,
- cerințe privind ciclul de viață al cheilor (creare, utilizare, revocare).

3.5.1 Standardele respectate în sistemul propus:

Aplicația noastră integrează explicit următoarele standarde:

- **RFC 9474** este implementat direct pentru semnăturile oarbe folosite în generarea credențialului anonim al alegătorului;
- **RFC 8017** este respectat în criptarea voturilor utilizând algoritmul RSA cu padding securizat, în conformitate cu schema **RSAES-OAEP**;
- **NIST SP 800-56B** este urmat parțial prin:
 - generarea automată de perechi unice de chei pentru fiecare autoritate electorală,
 - evitarea reutilizării cheilor între alegeri,
 - separarea logică între cheile de semnare și criptare (chiar dacă se folosește aceeași pereche RSA).

Aceste standarde contribuie la consolidarea securității și fiabilității sistemului de vot propus, permițând validare formală și auditabilitate externă, în conformitate cu bunele practici internaționale.

3.6 Comparație între tehnici criptografice utilizate în votul electronic

Sistemele de vot electronic pot fi construite folosind mai multe mecanisme criptografice, fiecare cu avantaje și limitări în ceea ce privește anonimitatea, verificabilitatea și complexitatea de implementare. În această secțiune sunt comparate două tehnici des utilizate în sistemele consacrate — criptarea ElGamal și rețelele de amestecare (mix-net-uri) — în raport cu abordarea adoptată în această lucrare, bazată pe semnături oarbe.

3.6.1 Criptare ElGamal

Criptosistemul ElGamal este preferat în aplicații precum Helios datorită proprietății sale omomorfe [Adi08]. Această caracteristică permite agregarea voturilor direct pe date criptate, evitând decriptarea individuală [Ben06]. Astfel, se pot calcula rezultate intermediare sau finale fără a compromite conținutul fiecărui vot în parte.

ElGamal este un criptosistem asimetric bazat pe dificultatea calculului logaritmului discret într-un grup ciclic. Algoritmul presupune următorii pași conform [Ben06]:

- Se alege un grup ciclic primitiv G de ordin q , cu generator g .
- Se generează cheia privată $x \in \mathbb{Z}_q$ și se calculează cheia publică $h = g^x$.
- Pentru a cripta un mesaj $m \in G$, se alege un număr aleator $r \in \mathbb{Z}_q$ și se calculează:

$$c_1 = g^r, \quad c_2 = m \cdot h^r \quad (3.14)$$

- Textul criptat este perechea (c_1, c_2) .
- Pentru decriptare, se calculează:

$$m = \frac{c_2}{c_1^x} = c_2 \cdot (c_1^x)^{-1} \quad (3.15)$$

Un avantaj major al schemei ElGamal este proprietatea sa de criptare omomorfă multiplicativă. Dacă două mesaje m_1 și m_2 sunt criptate separat, atunci produsul componentelor criptate (c_1, c_2) corespunde criptării produsului $m_1 \cdot m_2$. Această funcționalitate este utilizată pentru adunarea voturilor criptate într-un mod sigur și verificabil fără decriptare individuală.

Totuși, ElGamal nu oferă în mod nativ garanții de anonimitate. Deși criptarea protejează conținutul votului, ordinea în care sunt înregistrate voturile poate permite corelarea cu identitatea votantului, în special dacă se păstrează loguri de autentificare [Cha81]. De aceea, sistemele care utilizează ElGamal recurg frecvent la mix-net-uri pentru a introduce o reordonare anonimă înainte de decriptare.

3.6.2 Mix-net-uri

Mix-net-urile sunt protocoale criptografice utilizate pentru anonimizarea unui set de mesaje criptate [Cha81]. Fiecare server din lanțul de mixare aplică o permutare aleatoare și, eventual, recriptează voturile, astfel încât să fie imposibilă corelarea între mesajele de intrare și cele de ieșire. Pentru a garanta corectitudinea acestor operații,

mix-net-urile moderne furnizează dovezi criptografice de tip zero-knowledge (ZKP), ce pot fi verificate public [Joh06].

Formal, să considerăm un set de voturi criptate (c_1, c_2, \dots, c_n) unde fiecare c_i este o pereche ElGamal $(g^{r_i}, m_i \cdot h^{r_i})$. Un mix-server aplică o permutare aleatoare π și generează un set nou de voturi recriptate conform [Joh06] astfel:

$$c'_i = \text{Reencrypt}(c_{\pi(i)}) = (g^{r'_i} \cdot g^{r_{\pi(i)}}, m_{\pi(i)} \cdot h^{r'_i} \cdot h^{r_{\pi(i)}}) \quad (3.16)$$

Recriptarea păstrează conținutul votului dar schimbă complet forma sa criptată, asigurând astfel nedetectabilitatea legăturii dintre c_i și c'_i .

Pentru a preveni manipulările, mix-net-urile sunt însoțite de dovezi criptografice (ZKP) care atestă că permutarea și recriptarea au fost făcute corect, fără a dezvălui efectiv permutarea aleasă. Aceste dovezi sunt publice și verificabile, ceea ce asigură transparență și încredere în proces.

Deși oferă un nivel ridicat de anonimitate și verificabilitate universală, implementarea mix-net-urilor presupune o infrastructură criptografică sofisticată, costuri computaționale ridicate și o încredere distribuită între mai multe servere mixatoare. Aceste caracteristici le recomandă pentru alegeri naționale, dar le fac dificil de integrat în sisteme cu resurse limitate.

3.6.3 Compararea abordărilor

Pentru o sinteză clară, Tabelul 3.1 prezintă o comparație între abordarea folosită în această lucrare și alternativele consacrate, cu referințe la performanțele documentate în literatura de specialitate.

În mod particular, Benaloh [Ben06] oferă o analiză comparativă riguroasă asupra costurilor criptografice implicate în utilizarea mix-net-urilor bazate pe ElGamal. Sistemele cu mixare și recriptare oferă un nivel înalt de anonimitate și verificabilitate universală, dar presupun un timp de procesare semnificativ crescut în raport cu criptarea simplă. Timpul mediu de procesare per vot în astfel de arhitecturi este de ordinul sub-milisecundelor, în funcție de parametrii de prag (t) și optimizările implementării.

Tehnică	Anonimitate	Verificabilitate	Timp estimat per vot (ms)
ElGamal + mix-net (cu recriptare, $t = 3$)	Foarte ridicată	Universală	≈ 0.56
ElGamal (fără mix-net)	Limitată	Ridică	≈ 0.13

Tabela 3.1: Comparație între tehnici criptografice utilizate în votul electronic

Capitolul 4

Puterea de Vot – Fundamente Matematice, Statistice și Indici Cantitativi

4.1 Introducere

În sistemele democratice, votul fiecărui individ constituie fundamentul procesului decizional colectiv. Cu toate acestea, influența efectivă pe care un alegător o exercită asupra rezultatului final — cunoscută în literatura de specialitate drept *puterea de vot* — variază în funcție de arhitectura sistemului electoral. Analiza matematică și statistică a acestei puteri oferă o perspectivă riguroasă asupra echității și eficienței mecanismelor de vot, mai ales în contexte unde voturile pot avea ponderi diferite sau unde rezultatul depinde de formarea coalițiilor [AT02].

Deși aplicația implementată în cadrul acestei lucrări nu integrează în mod direct aceste modele, includerea lor în teză oferă o bază teoretică solidă pentru extinderi ulterioare — în special în direcția sistemelor de vot instituțional sau descentralizat (e.g., Decentralized Autonomous Organizations - DAOs), unde transparența și auditabilitatea influenței votanților sunt esențiale. În acest capitol, explorăm principalele modele cantitative de evaluare a puterii de vot, precum și aplicațiile lor potențiale în arhitecturi de vot electronic.

4.2 Modelarea Probabilistică a Puterii de Vot

Presupunând că alegătorii votează independent și cu șanse egale, *modelul de vot aleator* estimează puterea unui alegător i prin:

$$\text{Power}_i = \mathbb{P}(R = +1 \mid v_i = +1) - \mathbb{P}(R = +1 \mid v_i = -1) \quad (4.1)$$

Această formulă exprimă variația probabilității rezultatului global R atunci când un singur vot este modificat [AT02]. Se presupune că regula R este o funcție de agregare, de regulă semnul sumei ponderate a voturilor:

$$R(v_1, \dots, v_n) = \text{sign} \left(\sum_{i=1}^n w_i v_i - q \right) \quad (4.2)$$

unde w_i este ponderea votantului i , iar q este pragul de decizie. În votul electronic, această formulare permite evaluarea automată a impactului fiecărui vot, integrându-se în module de audit și transparență.

4.3 Vot Ponderat și Paradoxuri

Într-un sistem $[q; w_1, \dots, w_n]$, se consideră că o coaliție S este câștigătoare dacă $\sum_{i \in S} w_i \geq q$. Un votant este *decisiv* într-o coaliție dacă fără el coaliția pierde, iar cu el câștigă:

$$\sum_{j \in S \setminus \{i\}} w_j < q \leq \sum_{j \in S} w_j \quad (4.3)$$

Aceste configurații apar în sistemele de e-voting cu voturi instituționale sau în DAOs, unde ponderile pot reflecta contribuții financiare sau reputație. Evaluarea matematică a echilibrului acestor ponderi este crucială pentru evitarea manipulării rezultatelor.

4.4 Indici Cantitativi: Banzhaf și Shapley-Shubik

Indicele Banzhaf

Pentru fiecare subset $S \subseteq N \setminus \{i\}$, verificăm dacă i este decisiv în coaliția $S \cup \{i\}$. Numărul total de astfel de cazuri este η_i , iar indicele Banzhaf este:

$$\beta_i = \frac{\eta_i}{\sum_{j=1}^n \eta_j} \quad (4.4)$$

Acest indice măsoară proporția de cazuri în care votantul i are o influență decisivă. În sistemele electronice, acest calcul poate fi încorporat în raportările post-electorale pentru a oferi transparență asupra distribuției reale a puterii [AT02].

Pentru a înțelege modul în care indicele Banzhaf variază în funcție de ponderea unui alegător, considerăm un sistem simplu de vot cu 4 participanți, notat astfel:

$$[6; w_1, w_2, w_3, w_4] = [6; 4, 3, 2, 1] \quad (4.5)$$

unde $q = 6$ este pragul majorității și w_i sunt greutatea votanților. Obiectivul este să calculăm pentru fiecare alegător numărul de coaliții în care este decisiv.

Tabelul Coalițiilor Câștigătoare și Alegătorul Decisiv

Evaluăm toate subseturile de votanți, identificăm cele câștigătoare și determinăm dacă un votant este decisiv în acea coaliție (dacă eliminarea lui face coaliția pierzătoare).

Coaliție	Sumă Voturi	Câștigă?	Alegători Decisivi
{1,2}	7	Da	1,2
{1,3}	6	Da	1,3
{1,4}	5	Nu	-
{2,3}	5	Nu	-
{2,4}	4	Nu	-
{3,4}	3	Nu	-
{1,2,3}	9	Da	1,2
{1,2,4}	8	Da	1,2
{1,3,4}	7	Da	1,3
{2,3,4}	6	Da	2,3,4
{1,2,3,4}	10	Da	1,2

Calculul Indicelui Banzhaf

Numărăm de câte ori fiecare alegător este decisiv:

- Alegătorul 1 (pondere 4): decisiv în 5 coaliții
- Alegătorul 2 (pondere 3): decisiv în 4 coaliții
- Alegătorul 3 (pondere 2): decisiv în 3 coaliții
- Alegătorul 4 (pondere 1): decisiv în 1 coaliție

Indicele Banzhaf normalizat se obține împărțind fiecare valoare la totalul deciziilor ($5+4+3+1 = 13$):

$$\begin{aligned}\beta_1 &= \frac{5}{13} \approx 0.385 \\ \beta_2 &= \frac{4}{13} \approx 0.308 \\ \beta_3 &= \frac{3}{13} \approx 0.231 \\ \beta_4 &= \frac{1}{13} \approx 0.077\end{aligned}$$

Observații

Deși alegătorul 1 are doar dublul ponderii față de alegătorul 2 (4 vs. 2), el are o influență relativ mai mare. Totuși, creșterea ponderii nu duce întotdeauna la o creștere liniară a puterii. Aceasta evidențiază non-liniaritatea indicelui Banzhaf față de pondere.

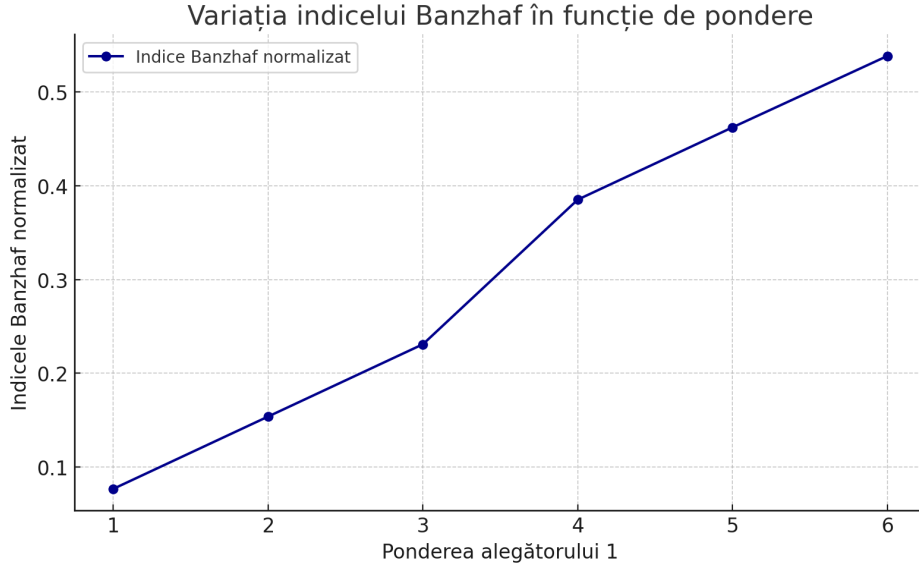


Figura 4.1: Variația indicelui Banzhaf al alegătorului 1 în funcție de ponderea sa, menținând restul constant. Se observă o creștere sub-liniară.

Indicele Shapley-Shubik

Fie π o permutare a alegătorilor. Votantul i este *pivot* dacă adăugarea sa într-o coaliție strict inferioară pragului q o transformă într-una câștigătoare. Indicele este:

$$\phi_i = \sum_{\pi \in \Pi} \frac{1}{n!} \cdot \mathbb{I}\{i \text{ este pivot în } \pi\} \quad (4.6)$$

unde \mathbb{I} este funcția indicator. Prin acest model, se cuantifică impactul marginal mediu al fiecărui alegător în toate scenariile posibile [AT02].

Pentru a înțelege modul în care indicele Shapley-Shubik funcționează, analizăm același sistem de vot:

$$[6; 4, 3, 2, 1]$$

Pentru fiecare permutare posibilă a celor patru alegători, identificăm *pivotul* — primul alegător care, adăugat unei coaliții parțiale, face ca suma voturilor să atingă sau să depășească pragul $q = 6$.

Permutări și Pivotalul fiecărei secvențe

Enumerăm toate cele $4! = 24$ permutări posibile și identificăm pivotalul:

Permutare	Pivot
1,2,3,4	1
1,2,4,3	1
1,3,2,4	1
1,3,4,2	1
1,4,2,3	1
1,4,3,2	1
2,1,3,4	2
2,1,4,3	2
2,3,1,4	3
2,3,4,1	3
2,4,1,3	3
2,4,3,1	3
3,1,2,4	3
3,1,4,2	3
3,2,1,4	3
3,2,4,1	3
3,4,1,2	3
3,4,2,1	3
4,1,2,3	3
4,1,3,2	3
4,2,1,3	3
4,2,3,1	3
4,3,1,2	3
4,3,2,1	3

Calculul Indicelui Shapley-Shubik

Numărăm de câte ori fiecare alegător este pivotalul (apare primul care atinge ≥ 6):

- Alegătorul 1: 6 ori
- Alegătorul 2: 2 ori
- Alegătorul 3: 12 ori
- Alegătorul 4: 4 ori

Calculăm indicele normalizat împărțind la numărul total de permutări (24):

$$\phi_1 = \frac{6}{24} = 0.25$$

$$\phi_2 = \frac{2}{24} = 0.083$$

$$\phi_3 = \frac{12}{24} = 0.50$$

$$\phi_4 = \frac{4}{24} = 0.167$$

Observații

În acest sistem, alegătorul 3 (cu pondere 2) ajunge frecvent în poziția de pivot deoarece completează coaliții parțiale spre pragul de 6. Spre deosebire de indicele Banzhaf, Shapley-Shubik e sensibil la ordinea de intrare și nu doar la ponderi absolute.

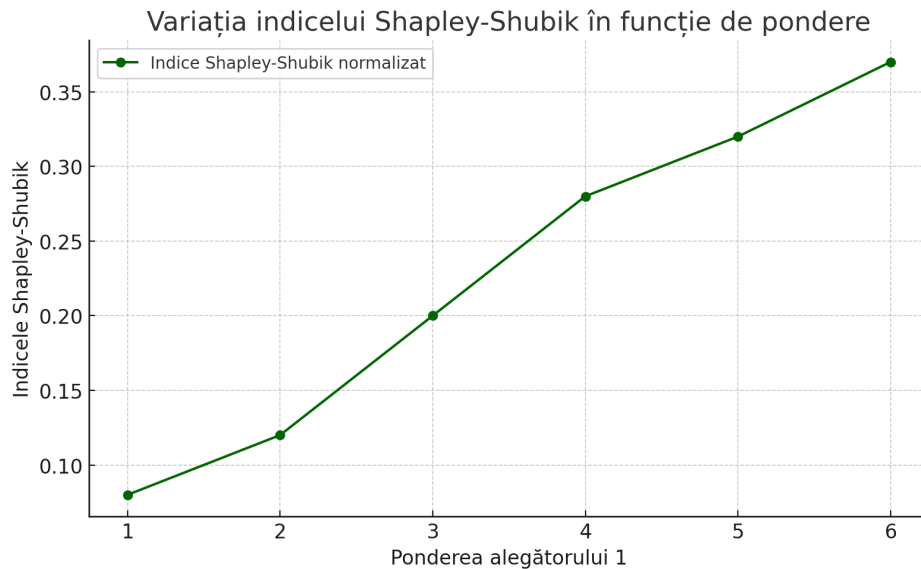


Figura 4.2: Variația indicelui Shapley-Shubik al alegătorului 1 în funcție de ponderea sa.

4.5 Aproximații și Teoreme

Când n este mare, calculul exact devine prohibitiv. În astfel de cazuri, se pot folosi rezultate asimptotice. Conform Penrose (1946), într-un sistem de vot pe două niveluri (e.g., colegii electorale), puterea unui alegător dintr-un district j este aproximativ:

$$\text{Power}_{ij} \propto \frac{w_j}{\sqrt{n_j}} \quad (4.7)$$

unde w_j este ponderea districtului și n_j este numărul de alegători. Această relație arată că pentru o reprezentare echitabilă, greutatea ar trebui scalată cu rădăcina pătrată a populației.[AT02; Pen46].

4.6 Simulări și Algoritmi Practici

Pentru a calcula sau aproxima indici de putere (precum Banzhaf sau Shapley-Shubik), sunt necesare metode computaționale adaptate dimensiunii sistemului de vot analizat. Într-un sistem electronic de vot, aceste simulări pot fi integrate ca module de analiză post-vot sau ca componente de audit[FM01; Bra07].

- **Enumerare brută:** constă în generarea tuturor celor 2^n subseturi posibile de alegători și evaluarea dacă un alegător este decisiv în fiecare subset. Această metodă este precisă, dar ineficientă pentru $n > 20$. Se aplică în sisteme cu număr mic de alegători sau atunci când se analizează structuri simple, precum consilii mici sau comitete.
- **Monte Carlo:** în locul evaluării tuturor subseturilor, se generează un eșantion aleator de coaliții. Se estimează frecvența cu care un alegător este decisiv în cadrul acestora. Această metodă reduce drastic timpul de calcul și oferă estimări acceptabile pentru n mare, cu un compromis între acuratețe și eficiență.
- **Aproximații analitice:** în unele cazuri, pot fi deduse formule închise sau asimptotice pentru indicii de putere, mai ales sub anumite distribuții ale greutăților (ex. uniforme, binomiale). Astfel de expresii sunt utile în proiectarea sistemelor sau pentru evaluări rapide fără simulări costisitoare.

În contextul votului electronic, aceste metode pot fi folosite pentru:

- validarea echilibrului între circumscripții;
- simularea impactului modificărilor structurale (ex. schimbarea pragului q);
- identificarea actorilor dominanți sau marginali într-un sistem descentralizat;
- analiza sensibilității sistemului la coaliții neprevăzute sau voturi strategice.

4.7 Modelarea Dependentei Voturilor și Preferințelor Latente

În realitate, votanții nu aleg complet independent. Ei sunt influențați de familie, prieteni, media, sau de trăsături comune geografice și socio-economice. Pentru a reflecta

aceste interdependențe, Gelman et al. propun două abordări matematice: una discretă și una continuă.[Gel+08; GH04]

4.7.1 Modelare Discretă a Dependenței Voturilor

Această abordare presupune că alegătorii formează o rețea (de exemplu, un arbore), în care fiecare nod reprezintă un votant. Alegerea fiecăruia depinde de vecinii săi. Matematic, se folosește o distribuție pe un graf $G = (V, E)$, modelând astfel:

$$\mathbb{P}(v_i \mid v_{\text{vecinii}(i)}) = \sigma \left(\sum_{j \in \text{vecinii}(i)} J_{ij} v_j + h_i \right) \quad (4.8)$$

unde σ este funcția logistică, J_{ij} sunt coeficienți de interacțiune (gradul de influență între alegători), iar h_i este o tendință individuală (bias). Această formulare seamănă cu modelul Ising din fizica statistică și permite simularea efectelor de contagiune ideologică sau polarizare.

Modelare Discretă a Dependenței Voturilor pe un Arbore de Influență

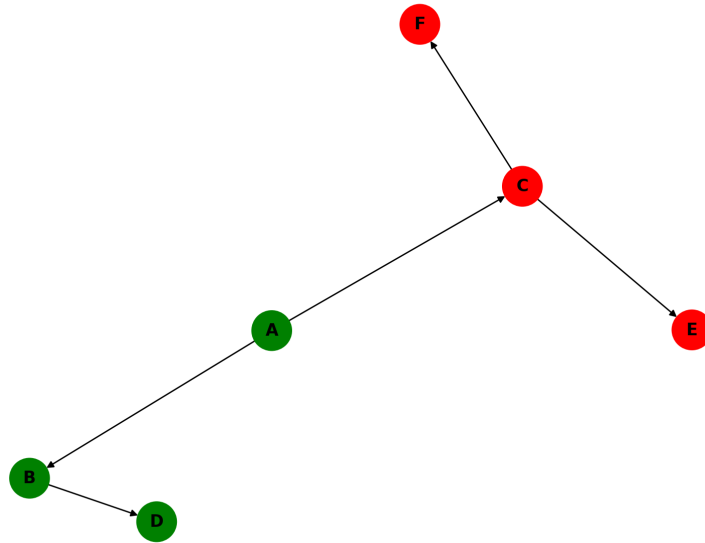


Figura 4.3: Modelare discretă a voturilor într-un sistem în care influența este transmisă pe un arbore. Alegătorii colorați în verde votează „pentru”, cei în roșu „împotriva”.

4.7.2 Modelare Continuă a Preferințelor Latente

Această abordare presupune că fiecare alegător are o preferință continuă, dar necunoscută x_i , iar votul efectiv este rezultatul acestei preferințe plus un zgomot aleator:

$$v_i = \text{sign}(x_i + \varepsilon_i) \quad (4.9)$$

unde $x_i \sim \mathcal{N}(\mu, \sigma^2)$ este preferința latentă, iar $\varepsilon_i \sim \mathcal{N}(0, \tau^2)$ este zgomotul. Aceasta permite captarea incertitudinii și a nehotărârii în alegeri. În practică, modelul poate fi calibrat folosind date reale (sondaje, voturi anterioare) și poate simula comportamentul colectiv într-un eșantion.

Un avantaj este că acest model generează automat corelații între voturi fără a presupune o rețea explicită. În sistemele de vot electronic, poate fi utilizat pentru:

- estimarea gradului de polarizare al electoratului;
- identificarea zonelor cu voturi incerte;
- anticiparea rezultatelor cu o distribuție de probabilitate, nu doar punctual.

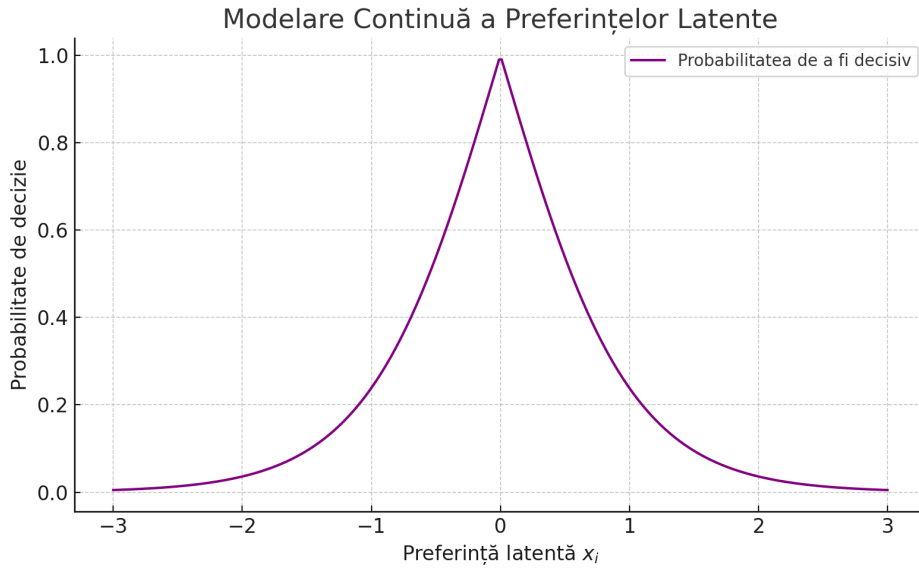


Figura 4.4: Probabilitatea ca un vot să fie decisiv în funcție de preferința latentă x_i . Alegătorii indeciși au o influență decisivă mai mare decât cei extrem de polarizați.

4.8 Modele Alternative: Corelare și Rețele

- **Modelul Ising:** simularea alegerii binare pe un graf $G = (V, E)$ unde votul unui nod depinde de vecinii săi [Gal08]. Energia totală:

$$H(v) = - \sum_{(i,j) \in E} J_{ij} v_i v_j - \sum_i h_i v_i \quad (4.10)$$

unde J_{ij} sunt coeficienți de influență și h_i bias-uri externe.

- **Regresii ierarhice:** modelare multi-nivel a probabilității de vot, utilă în predicție și analiză [GH07].

4.9 Aplicabilitate în Sisteme Electronice de Vot

Integrarea acestor metode permite:

1. Evaluarea echității între alegători în sisteme multi-districtuale.
2. Optimizarea regulilor de decizie în funcție de obiective democratice.
3. Audituri matematice ale sistemului (distribuție reală vs. ideală a puterii).
4. Configurarea în timp real a greutăților sau a normelor de consens în rețele de tip DAOs (Decentralized Autonomous Organizations).

Capitolul 5

Analiza comparativă

Acest capitol oferă o analiză aprofundată a mai multor sisteme de vot electronic, atât consacrate în literatura de specialitate, cât și al sistemului realizat în cadrul acestei lucrări. Analiza este structurată în jurul unor criterii fundamentale care reflectă cerințele esențiale ale unui sistem electoral modern: anonimitate, verificabilitate, securitate, auditabilitate, scalabilitate și complexitate de implementare. Obiectivul principal este acela de a înțelege punctele forte și limitările fiecărei soluții, dincolo de simpla funcționalitate tehnică.

5.1 Criterii de evaluare

Pentru a realiza o evaluare comparativă riguroasă, sistemele analizate au fost judecate în funcție de mai multe dimensiuni: nivelul de protecție al anonimatului votantului, posibilitatea verificării corectitudinii procesului electoral, robustețea criptografică, transparența și posibilitatea auditării externe, dificultatea de implementare, capacitatea de scalare și caracterul deschis al codului sursă.

5.2 Sistemul Helios

Helios este un sistem de vot online open-source, conceput pentru alegeri în medii controlate precum universități sau organizații. Acesta utilizează criptografie omomorfă și dovezi zero-knowledge pentru a asigura verificabilitatea end-to-end. Voturile sunt criptate local de către alegători și publicate într-un registru public, permițând oricărui utilizator să verifice prezența propriului vot. Cu toate acestea, lipsa mecanismelor de prevenire a coerciției și dependența de autorități mix-net pentru anonimizare limitează aplicabilitatea Helios în alegeri la scară națională.[Adi08]

Caracteristici cheie Helios:

- Criptare omomorfă ElGamal cu dovezi zero-knowledge;

- Registru public pentru verificare universală;
- Lipsă de *receipt-freeness*, vulnerabilitate la coerciție;
- Ideal pentru alegeri academice sau organizaționale.

5.3 Sistemul Estonia i-Voting

Estonia i-Vote este singurul sistem implementat pe scară națională în alegeri parlamentare. Votul este exprimat online, autentificat printr-un ID digital, și semnat digital de alegător. Sistemul permite revotarea, garantând că doar ultimul vot este considerat. Verificarea se face printr-o aplicație mobilă. Deși eficient și bine integrat cu infrastructura digitală a statului, sistemul nu oferă anonimat complet și este vulnerabil la atacuri asupra dispozitivului personal al alegătorului.[Est17]

Caracteristici cheie Estonia i-Vote:

- Integrare completă cu sistemul de identitate digitală națională;
- Semnătură digitală obligatorie și verificare prin aplicație mobilă;
- Revotare posibilă, votul fizic suprascrie cel electronic;
- Anonimitate relativă, dar scalabilitate excelentă.

5.4 Sistemul REVS

Robust Electronic Voting System(REVS) este un sistem distribuit orientat spre reziliență și anonimitate completă. El separă componentele de validare și colectare a voturilor și utilizează semnături oarbe pentru a preveni orice asociere între votant și vot. Sistemul este tolerant la defecțiuni, acceptând voturi semnate de o majoritate de validatori, chiar dacă unii sunt compromiși. Este ideal pentru contexte cu amenințări ridicate la adresa securității.[SR21]

Caracteristici cheie REVS:

- Semnături oarbe pentru anonimitate perfectă;
- Arhitectură distribuită: *Validator*, *Ballot Box*, *Tallyer*;
- Reziliență la defecțiuni și validatori compromiși;
- Ideal pentru alegeri desfășurate în medii nesigure.

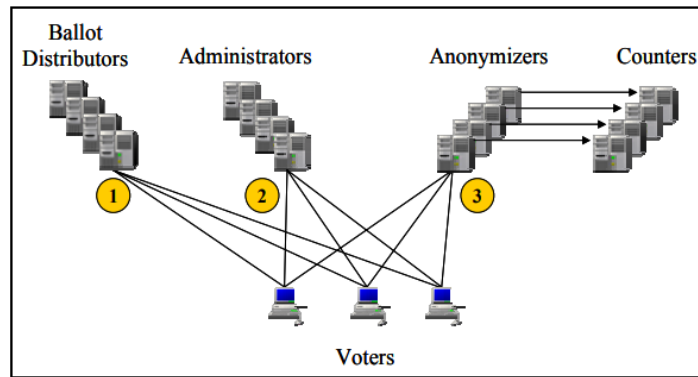


Figura 5.1: Arhitectura sistemului REVS

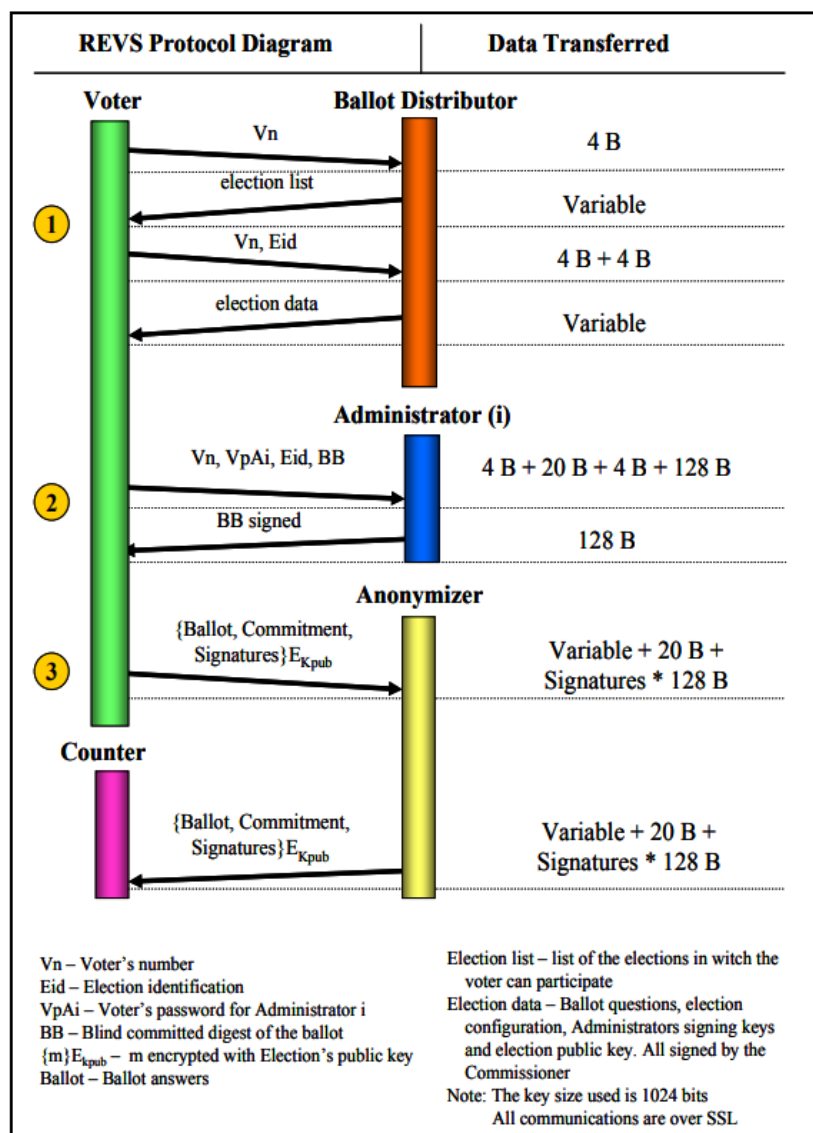


Figura 5.2: Diagrama de protocol în REVS

Capitolul 6

Arhitectura sistemului de vot anonim

6.1 Prezentare generală

Sistemul propus adoptă o arhitectură de tip **client-server**, structurată pe mai multe straturi funcționale care separă responsabilitățile între interfața utilizator, logica aplicației și infrastructura de stocare. Această decuplare oferă o mai bună scalabilitate, o mentenanță mai ușoară și o protecție eficientă a datelor sensibile, esențială într-un context de vot electronic anonim.

6.2 Arhitectura pe straturi

Aplicația este organizată conform unui model arhitectural stratificat (layered), inspirat din arhitectura MVC extinsă, care separă clar responsabilitățile între interfață, controlere, logica de business, criptografie și accesul la date.

- **Presentation Layer (Frontend)** – include interfața web realizată cu HTML/CSS, JavaScript. Aceasta permite alegătorilor să se autentifice, să solicite tokenuri anonime și să voteze, precum și organizatorilor să creeze și să monitorizeze alegeri.
- **Controller Layer** – conține clasele REST precum `ElectionController`, `VoterController`, `BlindSignatureController`, care preiau cererile HTTP, gestionează rutarea și transformă datele primite în DTO-uri.
- **Service Layer** – implementează logica principală a aplicației, incluzând gestionarea alegerilor, generarea tokenurilor anonime, criptarea voturilor, validarea și procesarea rezultatelor. Clasele precum `ElectionService`, `VoteService` sau `BlindSignatureService` centralizează funcționalitatea critică.

- **Cryptography Layer** – strat logic izolat, care conține clase precum `RSAKeyManager` și `BlindSignatureUtils`, responsabile pentru criptarea RSA, generarea și verificarea semnăturilor oarbe, în conformitate cu RFC 9474 și RFC 8017.
- **Repository Layer** – gestionează accesul la baza de date prin Spring Data JPA. Include repository-uri precum `ElectionRepository`, `CandidateRepository` sau `BlindCredentialRepository`, care oferă metode declarative pentru manipularea entităților persistente.
- **Database Layer** – reprezintă stocarea fizică a datelor într-o bază PostgreSQL. Datele sunt organizate în tabele normalizate, separate între alegători, voturi (criptate), candidați, autorități electorale și credențiale anonime.

Componente auxiliare: În afara acestor straturi logice, sistemul include și componente de infrastructură, cum ar fi `RunoffElectionScheduler`, plasat în pachetul `utils`, care rulează periodic și declanșează automat generarea alegerilor de tip `TOP_TWO_RUNOFF`, apelând metode din `ElectionService`. Această componentă nu constituie un strat propriu-zis, ci o piesă de automatizare tehnică.

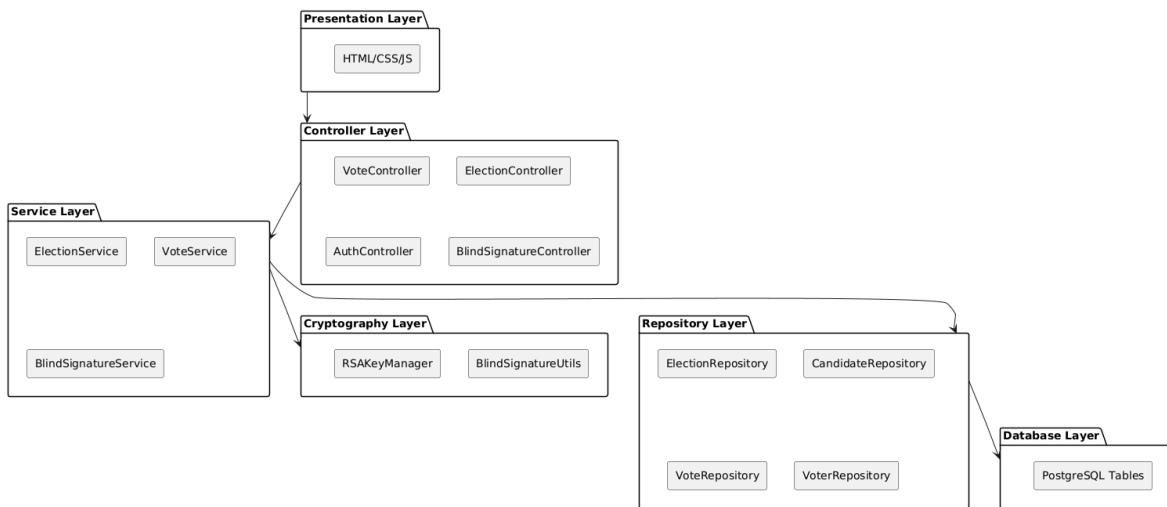


Figura 6.1: Arhitectura logică pe straturi a aplicației

6.3 Modelul bazei de date

Baza de date utilizată este PostgreSQL și stochează toate datele legate de alegeri, voturi, candidați, alegători și autoritățile electorale. Structura este concepută astfel încât să respecte principiile de normalizare și să asigure separarea completă între identitatea votantului și votul exprimat.

6.3.1 Entități principale

- **Voter** – conține informații minime despre alegător (ex: UUID, voterName, voterEmail, region, etc.);
- **Election** – detalii despre alegeri (denumire, perioadă, cine a creat alegerea);
- **Candidate** – numele și identificatorii candidaților asociați cu o alegere;
- **Vote** – stochează voturile criptate și nu conține referințe către votant;
- **ElectionAuthority** – entitate care gestionează semnăturile oarbe și cheia privată;
- **BlindCredential** – token semnat prin semnătură oarbă, utilizat la exprimarea votului.

6.3.2 Principii de proiectare

- **Separarea logică între votant și vot:** tabela *Vote* nu conține niciun ID de votant;
- **Utilizarea cheilor externe și UUID-uri** pentru evitarea expunerii datelor sensibile;
- **Semnătura oarbă** este stocată în forma credențialului anonim, fără a permite corelarea înapoi cu alegătorul;
- **Stocarea criptată a voturilor**, direct în baza de date.

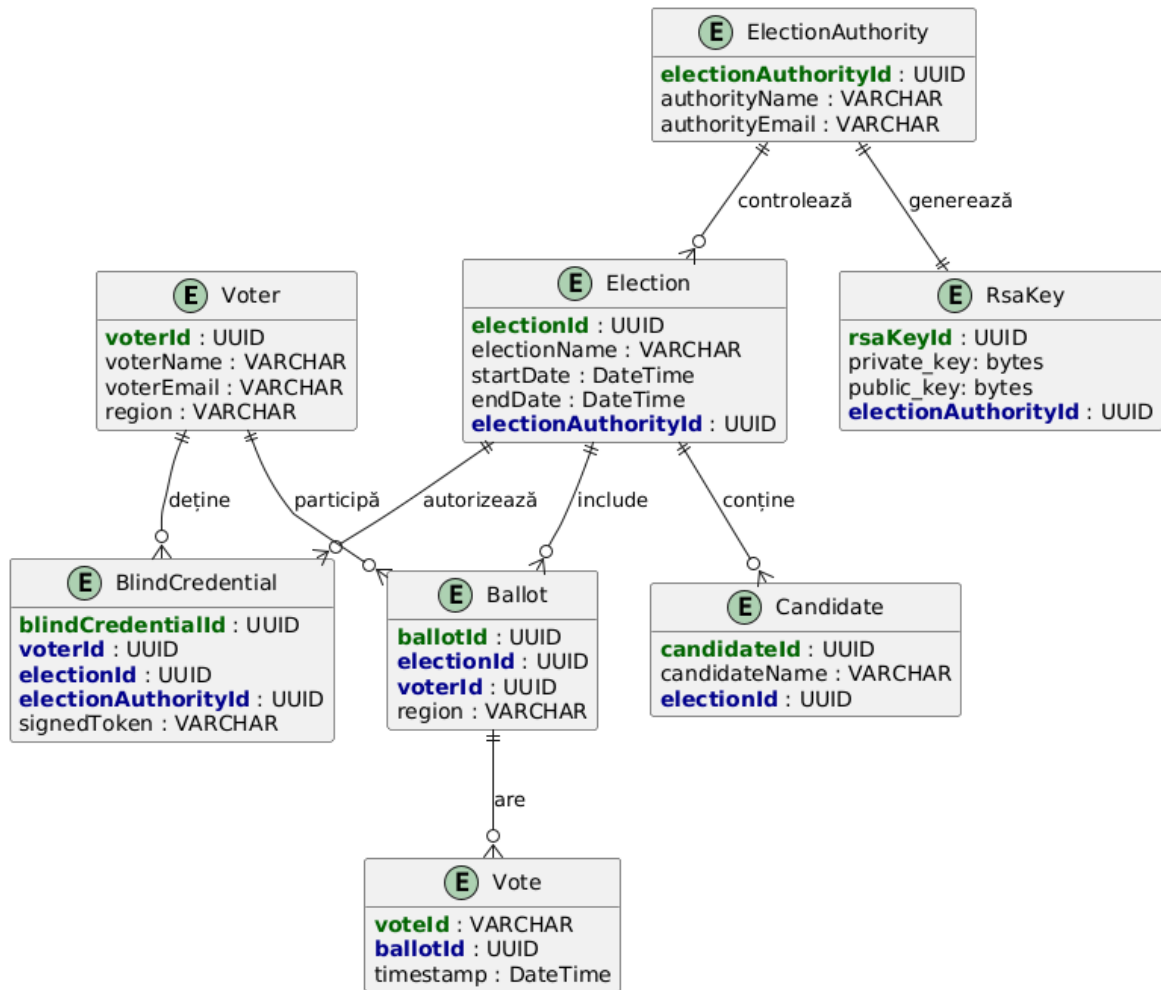


Figura 6.2: Arhitectura bazei de date a sistemului de vot anonim

6.4 Modelul domeniului și diagrama de clase

Modelul de domeniu este alcătuit din entități care reflectă realitatea aplicației și permit manipularea logicii de afaceri într-un mod coerent și extensibil.

Entități principale

- **Voter** – reprezintă un alegător înregistrat în sistem. Conține un UUID, un hash al adresei de e-mail, tipul de alegător (**BASIC** sau **INSTITUTION_VERIFIED**), calea către o imagine de profil și opțional regiunea și ziua de naștere.
- **Election** – definește o alegere electronică, cu detalii precum denumirea, tipul (**STANDARD**, **POLL**, **TOP_TWO_RUNOFF**), perioada de desfășurare și nivelul de acces (**BASIC** sau **INSTITUTION**).
- **Candidate** – reprezintă un candidat asociat unei alegeri.
- **Vote** – stochează votul propriu-zis, în formă criptată, fără nicio referință la identitatea votantului. Include și momentul votării.
- **BlindCredential** – token-ul anonim generat prin semnătură oarbă, utilizat pentru a valida dreptul de vot fără a compromite anonimatul.
- **ElectionAuthority** – entitate care deține cheia RSA pentru semnarea tokenurilor anonime și gestionează validarea alegătorilor.
- **RsaKey** – obiect care conține cheia publică și cheia privată (criptată) asociate unei autorități.
- **Ballot** – structură care descrie selecția votantului (una sau mai multe opțiuni) exprimată într-o alegere.

6.4.1 Principii de proiectare

Structura claselor reflectă mai multe principii solide de proiectare:

- **Encapsularea logicii de business** în clasele de domeniu, fără dependență directă de controlere sau servicii;
- **Separarea anonimatului** – prin faptul că **Vote** nu este în relație directă cu **Voter**;
- **Modularitate** – fiecare clasă are o responsabilitate clară și poate fi testată izolat;
- **Utilizarea UUID-urilor** ca identificatori standard pentru entități;

- Respectarea SRP (Single Responsibility Principle) – clasele sunt scurte, orientate pe scopuri unice.

6.4.2 Diagramă de clase

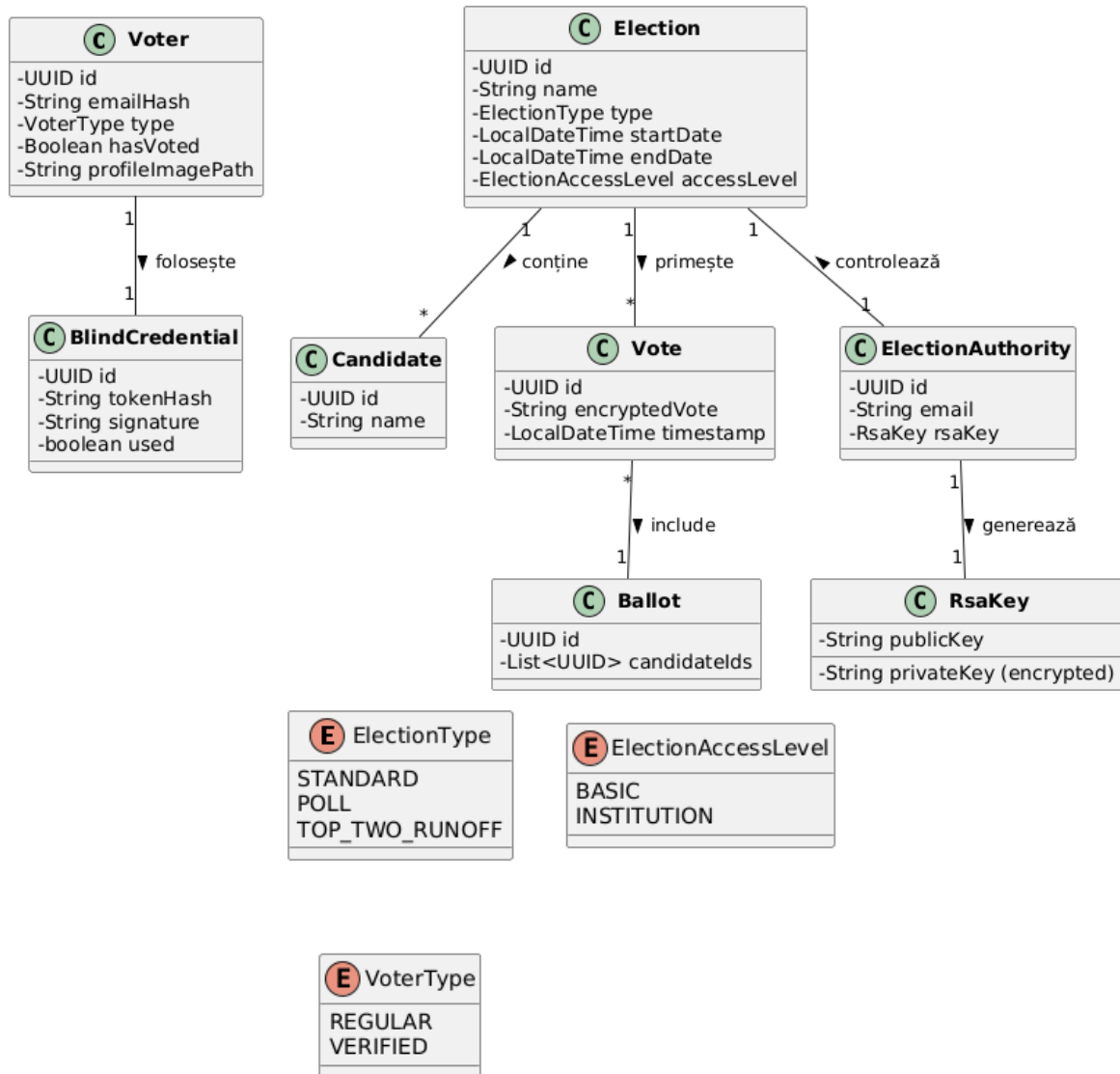


Figura 6.3: Diagrama de clase pentru modelul de domeniu

6.4.3 Fluxul de vot anonim

Pentru a garanta anonimatul și integritatea fiecărui vot, procesul de votare este structurat într-un flux clar, cu pași bine definiți. Sistemul combină verificarea eligibilității cu un mecanism criptografic bazat pe semnături oarbe și criptare RSA, fără a stoca nicio legătură între alegător și opțiunea de vot exprimată.

Pașii fluxului de vot anonim:

- **1. Autentificare:** Alegătorul se conectează în platformă și este identificat prin credențiale valide.
- **2. Verificare eligibilitate:** Sistemul verifică dacă alegătorul este autorizat să voteze, în funcție de tipul alegerii (BASIC sau INSTITUTION).
- **3. Solicitare token anonim:** Alegătorul trimite o cerere pentru un token blindat (orbit), care este semnat de autoritatea electorală folosind semnătură oarbă (blind signature), fără a cunoaște conținutul cererii.
- **4. Exprimarea votului:** După obținerea tokenului semnat, utilizatorul completează buletinul de vot și trimite opțiunea aleasă împreună cu tokenul anonim.
- **5. Validare:** Serverul verifică autenticitatea semnăturii oarbe și dacă tokenul nu a mai fost utilizat.
- **6. Criptare și stocare:** Dacă validarea este reușită, votul este criptat cu cheia publică RSA a alegerii și stocat în siguranță în baza de date. Tokenul este marcat ca "utilizat".
- **7. Feedback către utilizator:** Sistemul răspunde cu succes sau eroare, în funcție de validarea tokenului și de criptarea reușită.
- **8. Actualizare rezultate:** Panoul organizatorului se actualizează în timp real prin WebSocket, fără a compromite confidențialitatea.

Întregul proces este conceput astfel încât să asigure:

- imposibilitatea corelării unui vot cu un alegător;
- protejarea conținutului votului în tranzit și în stocare;
- prevenirea fraudelor prin validarea unică a tokenului anonim.

Capitolul 7

Implementarea sistemului de vot electronic

Acest capitol descrie modul concret în care a fost realizată aplicația propusă pentru vot electronic. Implementarea acoperă atât partea de server (backend), cât și interfața cu utilizatorul (frontend), folosind tehnologii moderne care oferă securitate, modularitate și scalabilitate. Sunt prezentate funcționalitățile cheie dezvoltate, precum și structura generală a aplicației.

7.1 Tehnologiile utilizate

Alegerea componentelor software s-a făcut având în vedere maturitatea tehnologiilor, suportul pentru criptografie și integrarea facilă între straturi. Mai jos sunt prezentate componentele majore:

- **Frontend-ul (client web)** este realizat folosind HTML, CSS și JavaScript, cu Ajax pentru apelurile asincrone. Este minimalist, concentrându-se pe accesibilitate și funcționalitate. Interfața permite autentificarea, obținerea tokenului anonim și trimiterea buletinului de vot.
- **Backend-ul (server)** este implementat în **Java 17** folosind **Spring Boot 3.2**. Această alegere oferă un cadru stabil, modular și extensibil pentru dezvoltarea rapidă a aplicațiilor REST. Datorită ecosistemului Spring, sunt integrate cu ușurință componente precum validatori, controlere, WebSocket și ORM (JPA-/Hibernate).
- **Baza de date PostgreSQL 15** este utilizată pentru stocarea persistentă a datelor. PostgreSQL a fost ales pentru suportul robust pentru tipuri de date criptate, integritate tranzacțională și suport extins pentru UUID și JSON.

- **WebSocket-ul** este implementat prin modulul **spring-websocket** și permite trimiterea în timp real a actualizărilor privind rezultatele votului, fără a fi nevoie de reîncărcarea paginii.
- **Modulul criptografic** utilizează algoritmul RSA cu implementare custom, bazat pe specificațiile **RFC 8017 (PKCS #1)**. Generarea de chei, semnăturile digitale și semnăturile oarbe sunt tratate în clase dedicate. Cheile RSA sunt generate pe 2048 biți și gestionate pentru fiecare autoritate electorală.
- **Semnăturile oarbe** sunt implementate conform **RFC 9474**, într-un modul izolat, ce permite orbirea, semnarea și dezorbirea în siguranță, fără ca autoritatea să cunoască conținutul tokenului.
- **Gestionarea fișierelor și a imaginilor** (pentru profiluri de utilizator) este realizată local, folosind sistemul de fișiere al serverului, într-un director securizat.

Componentă	Versiune
Java	17
Spring Boot	3.2.x
PostgreSQL	15.x
Spring WebSocket	integrat în Spring Boot
JPA + Hibernate	latest via Spring Boot
Librării crypto	Java Security + custom RSA

Tabela 7.1: Versiunile tehnologiilor utilizate în sistem

7.2 Funcționalități implementate

Această secțiune descrie principalele funcționalități implementate în sistemul de vot electronic, alături de explicații vizuale și fluxuri specifice. Pentru fiecare funcționalitate majoră sunt prezentate pașii interni și interacțiunile cu utilizatorul sau cu alte componente ale aplicației.

7.2.1 Înregistrare și autentificare

Funcționalitatea de înregistrare permite utilizatorilor să își creeze conturi folosind adresa de email, o parolă sigură și numele. Parolele sunt criptate cu BCrypt înainte de a fi stocate în baza de date. La autentificare, credențialele sunt verificate și utilizatorul este direcționat către pagina principală a aplicației.

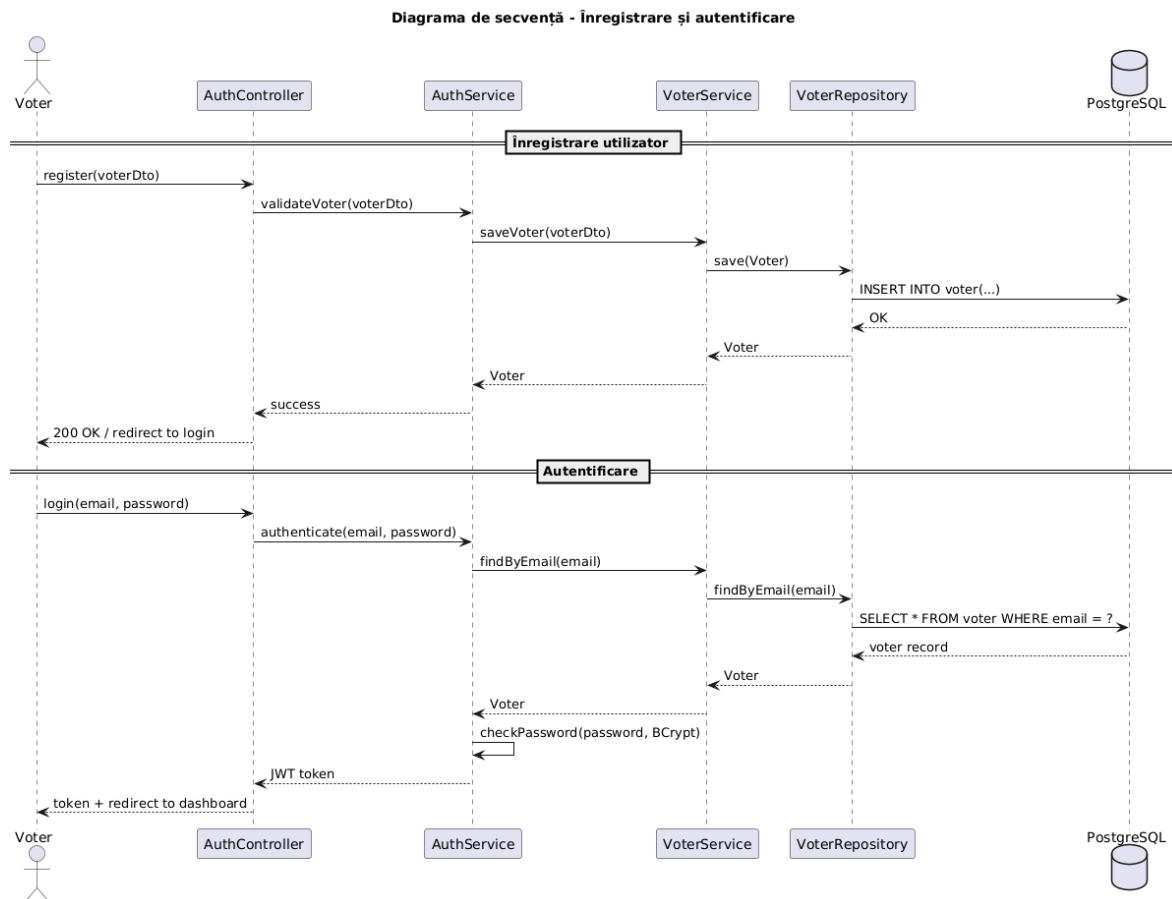
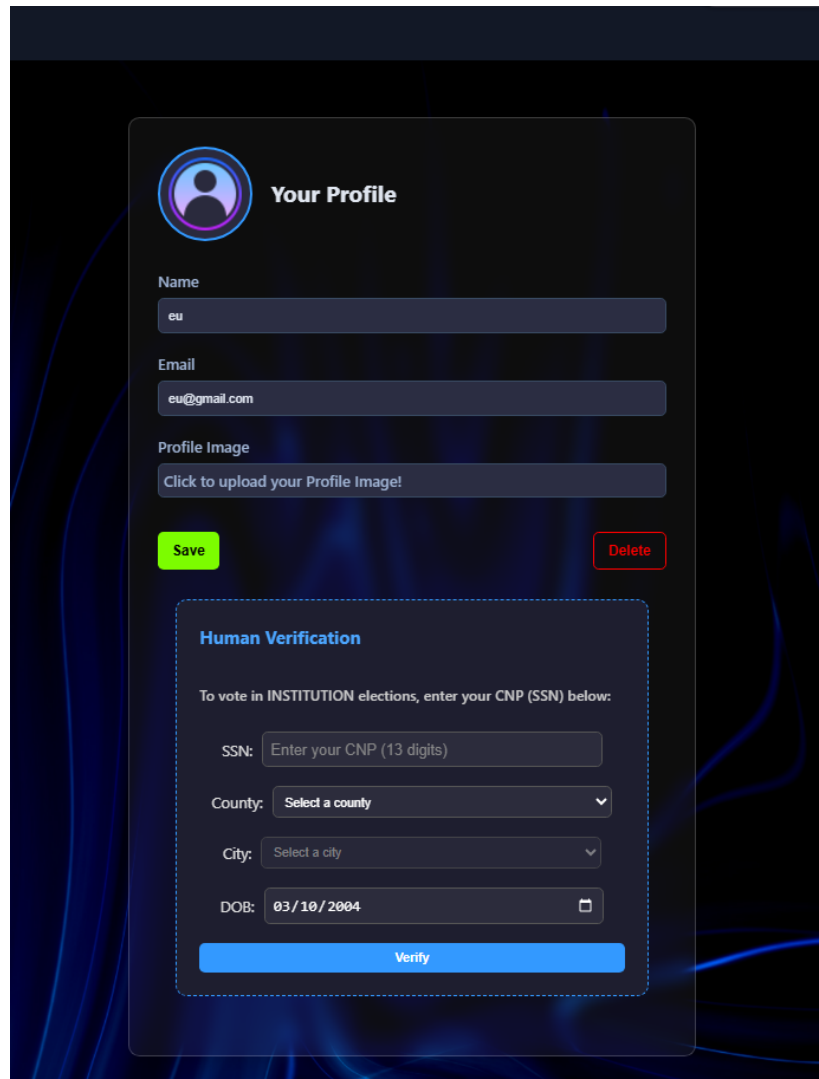


Figura 7.1: Diagramă de secvență pentru înregistrare și autentificare

7.2.2 Verificarea identității

Organizatorii pot fi de doua tipuri: utilizatori normali sau instituții certificate. În cazul celui de-al doilea tip, votanții trebuie să își valideze profilul pentru a putea participa în cadrul alegerilor. Aceștia sunt rugați să introducă CNP-ul alături de data de naștere și domiciliul.



The image shows a web interface for profile verification. At the top, there's a 'Your Profile' section with a circular profile icon placeholder. Below it are input fields for 'Name' (containing 'eu') and 'Email' (containing 'eu@gmail.com'). There's also a 'Profile Image' section with a button that says 'Click to upload your Profile Image!'. At the bottom of this section are two buttons: a green 'Save' button and a red 'Delete' button. Below these is a dashed-line box titled 'Human Verification'. Inside this box, it says 'To vote in INSTITUTION elections, enter your CNP (SSN) below:'. There are four input fields: 'SSN:' with a placeholder 'Enter your CNP (13 digits)', 'County:' with a dropdown menu showing 'Select a county', 'City:' with a dropdown menu showing 'Select a city', and 'DOB:' with a date field showing '03/10/2004' and a calendar icon. At the bottom of the dashed box is a blue 'Verify' button.

Figura 7.2: Validarea profilului

7.2.3 Gestionarea alegerilor

Organizatorii pot crea și edita alegeri folosind o interfață intuitivă care include:

- completarea titlului, descrierii și tipului de alegere;
- setarea unei parole;
- selecția datelor de început și sfârșit;
- definirea listei de candidați;

Tipurile de alegeri care pot fi utilizate sunt următoarele: **STANDARD** (folosit pentru a predefini numărul de voturi per candidat), **POLL** (folosit pentru multiple voturi), **TWO_TOP_RUNOFF** (folosit pentru alegeri de tip prezidențial, după terminarea primului tur sistemul creează automat turul doi în funcție de datele calendaristice introduse).

Figura 7.3: Panoul de creare a unei alegeri

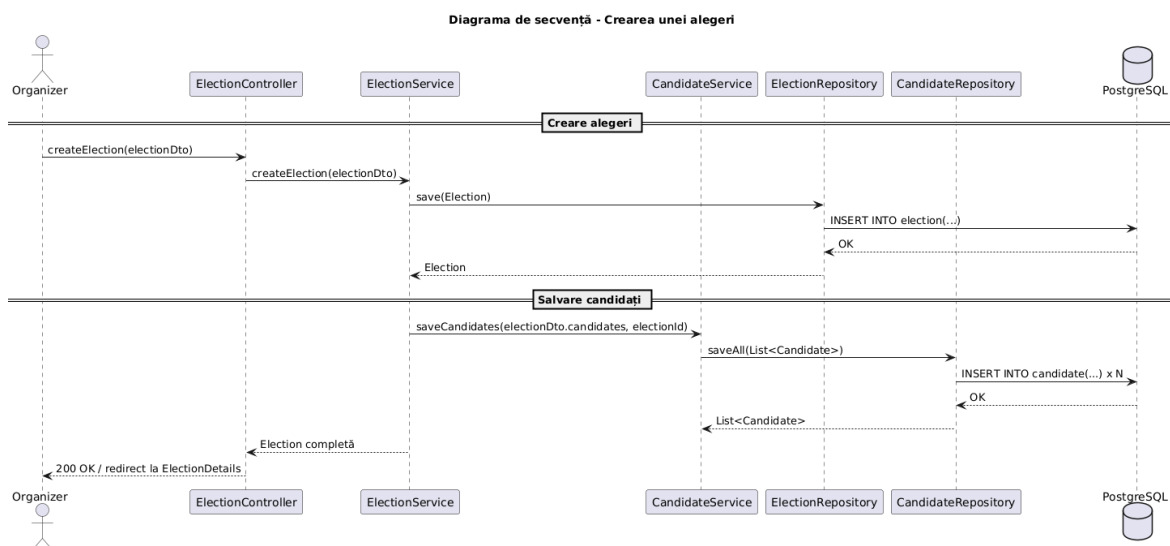


Figura 7.4: Diagramă de secvență pentru crearea unei alegeri

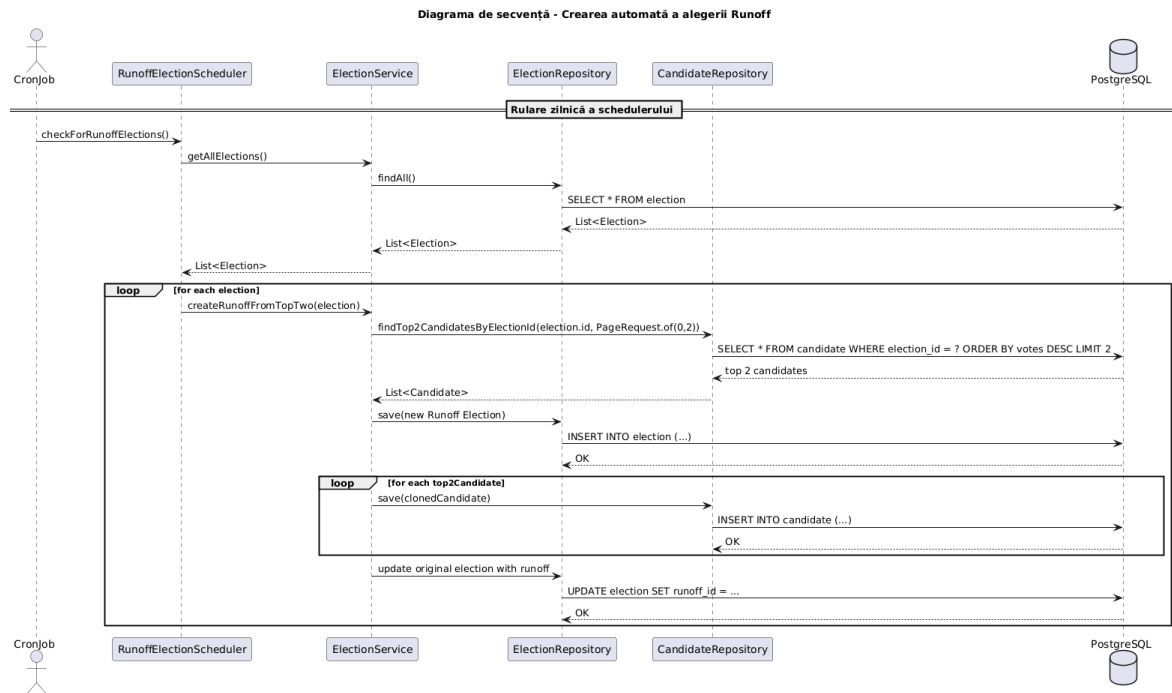


Figura 7.5: Diagramă de secvență pentru crearea turului doi in cazul TOP_TWO_RUNOFF

7.2.4 Mecanismul de votare anonimă

Votarea se desfășoară printr-un protocol care asigură separarea identității de alegere:

- Alegătorul autentificat solicită un token anonim (orbit);
- Serverul validează eligibilitatea și semnează tokenul folosind semnătură oarbă;
- Alegătorul își exprimă votul și trimite opțiunea criptată împreună cu tokenul;
- Serverul validează semnătura și salvează votul dacă tokenul este valid și nefolosit.

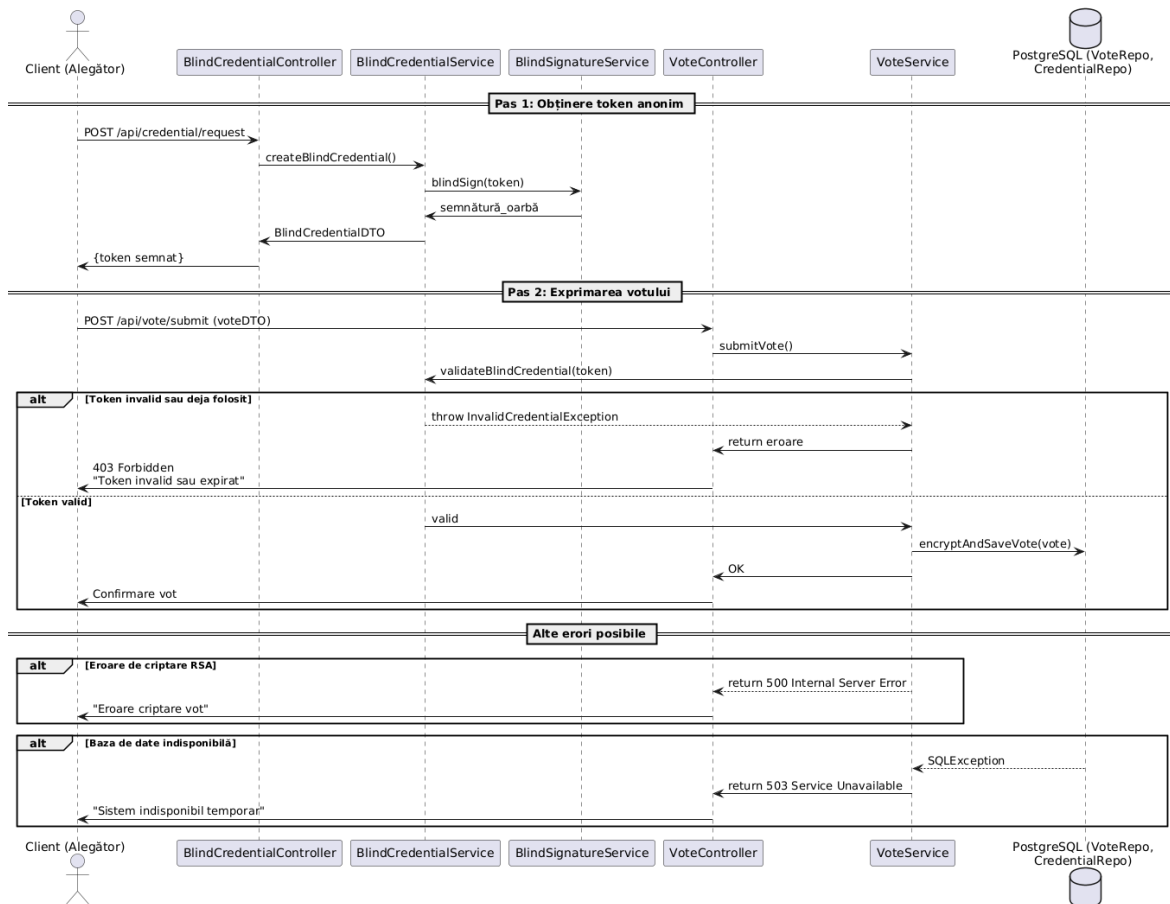


Figura 7.6: Diagrama de secvență a mecanismului de vot anonim

7.2.5 Numărarea voturilor în timp real și finală

Procesul de numărare a voturilor este împărțit în două faze distincte: colectarea și agregarea în timp real (pe durata alegerii), urmată de decriptarea și afișarea finală a rezultatelor, odată cu încheierea perioadei de votare.

1. Pe durata desfășurării votului

- Sistemul înregistrează fiecare vot criptat imediat după depunere;
- Rezultatele parțiale (numărul de voturi exprimate per candidat) sunt agregate în mod anonim și transmise în timp real, fără a compromite conținutul votului;
- Interfața utilizatorului afișează dinamica votului în baza acestor statistici temporare;
- Aceste date nu permit deducerea preferințelor individuale și nu implică decriptarea voturilor.

2. După încheierea perioadei de votare

- Se colectează toate voturile criptate, stocate în mod anonim;
- Voturile valide sunt decriptate folosind cheia privată asociată alegerii;
- Rezultatele finale sunt calculate prin agregarea opțiunilor exprimate și publicate în mod transparent;

Panourile se actualizează în timp real prin WebSocket, afișând: numărul de voturi per candidat, dinamica voturilor pe intervale de timp și zonele din care s-a votat.

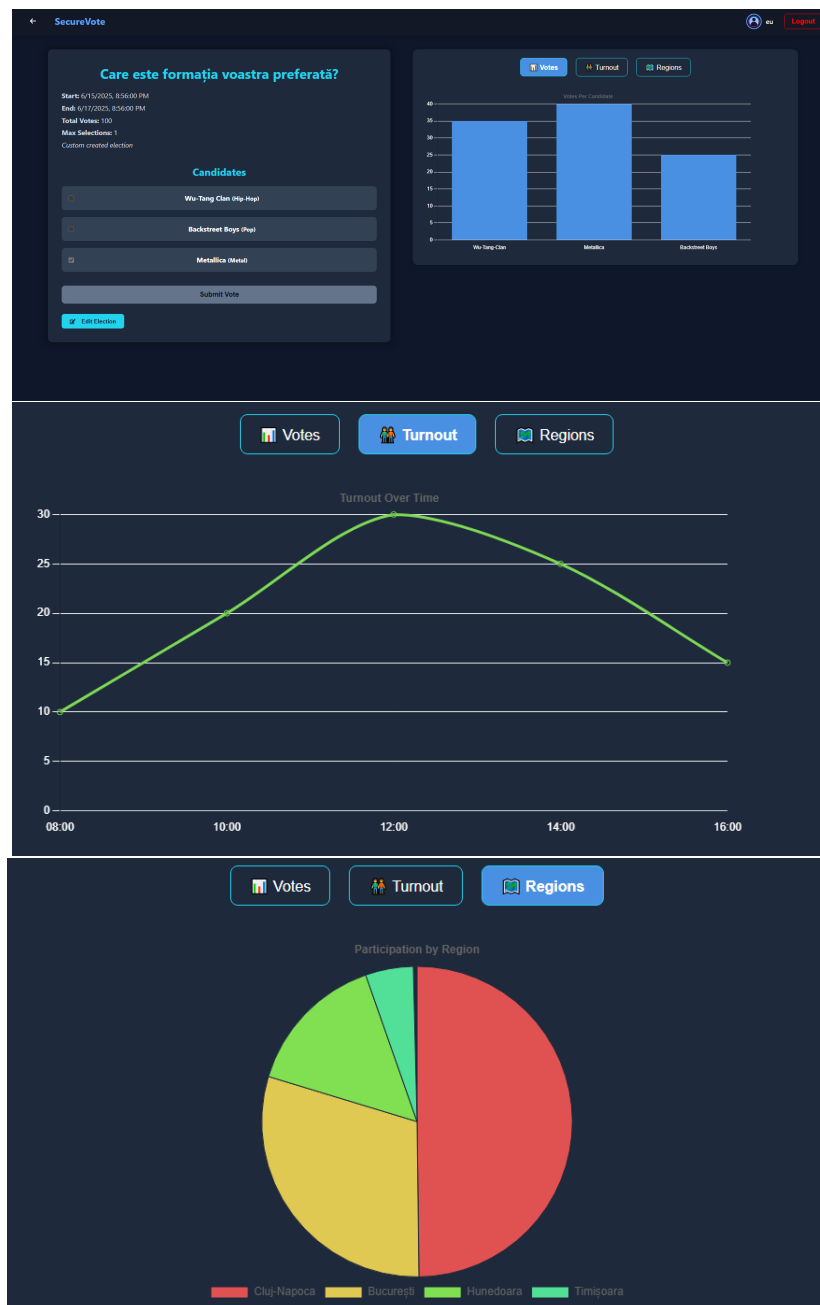


Figura 7.7: Panoul de rezultate în timp real pentru votanți

7.2.6 Administrare

Funcționalitățile administrative permit organizatorilor:

- să editeze alegeri existente;
- să adauge, modifice sau șteargă candidați;
- să configureze rapid parametrii unei alegeri în funcție de scenariu;

Nu a fost implementat un modul de audit sau export de date, dar interfața admin este funcțională și extensibilă.

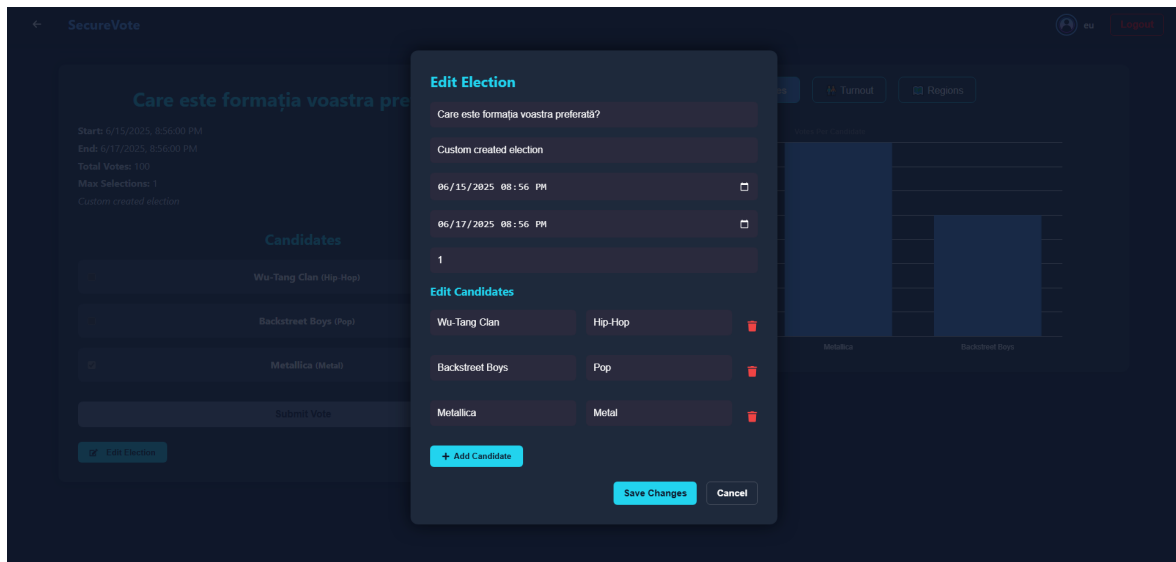


Figura 7.8: Editarea candidaților într-o alegere existentă

7.3 Criptarea în sistemul de vot electronic

Sistemul utilizează criptografie asimetrică RSA, implementată conform specificațiilor **RFC 8017**, pentru a asigura confidențialitatea voturilor. Fiecare alegere este asociată cu o pereche unică de chei RSA generată la inițializare.

7.3.1 Structura modulelor criptografice

Funcționalitatea criptografică este distribuită în următoarele clase:

KeyGenerationService.java – generează o pereche RSA (2048 biți) pentru fiecare autoritate electorală:


```

KeyPairGenerator keyPairGenerator = KeyPairGenerator.
    getInstance("RSA");
keyPairGenerator.initialize(2048);
KeyPair keyPair = keyPairGenerator.generateKeyPair();

```

EncryptionService.java – extrage componentele cheii publice și semnează mesaje orbite:

```

public Map<String, String> extractPublicKeyComponents(RsaKey
    rsaKey)
public String signBlindedMessage(BigInteger blindedMessage,
    UUID electionId)

```

VoteService.java – criptează voturile și le salvează anonim:

```

Cipher cipher = Cipher.getInstance("RSA");
cipher.init(Cipher.ENCRYPT_MODE, publicKey);
byte[] encryptedVote = cipher.doFinal(voteContent.getBytes());

```

EncryptionController.java – expune endpointuri REST pentru semnarea mesajelor orbite și publicarea cheilor publice.

7.3.2 Etapele procesului criptografic

Fluxul de criptare a votului este următorul:

1. **Inițializare:** `KeyGenerationService` creează o pereche RSA unică și o asociază unei alegeri.
2. **Orbirea mesajului:** utilizatorul generează local un mesaj orbit $m' = m \cdot r^e \bmod n$ (în afara aplicației).
3. **Semnarea orbă:** `EncryptionController` primește m' și folosește funcția: `EncryptionService.signBlindedMessage()` pentru a aplica semnătura cu cheia privată.
4. **Dezorbirea:** utilizatorul dezorbeste semnătura și obține un token anonim validat.
5. **Criptarea votului:** în `VoteService`, opțiunile alese (ID-urile candidaților) sunt convertite într-un string și criptate cu cheia publică a alegerii:

```

cipher.init(Cipher.ENCRYPT_MODE, publicKey);
byte[] encryptedVote = cipher.doFinal(voteContent.
    getBytes(StandardCharsets.UTF_8));

```

6. **Stocarea votului:** votul criptat este salvat fără nicio legătură cu identitatea utilizatorului.
7. **Numărarea:** la finalul alegerii, voturile sunt decriptate în `VoteService` folosind: `VoteService.decryptAndTallyVotes()`.

```
cipher.init(Cipher.DECRYPT_MODE, privateKey);
byte[] decryptedBytes = cipher.doFinal(vote.
    getEncryptedVote());
```

7.3.3 Separarea identității de conținutul votului

Semnătura oarbă implementată în `EncryptionController` și `EncryptionService` permite validarea eligibilității fără a expune identitatea votantului. **Tokenul semnat orb** este folosit o singură dată și nu este legat în niciun fel de datele de autentificare.

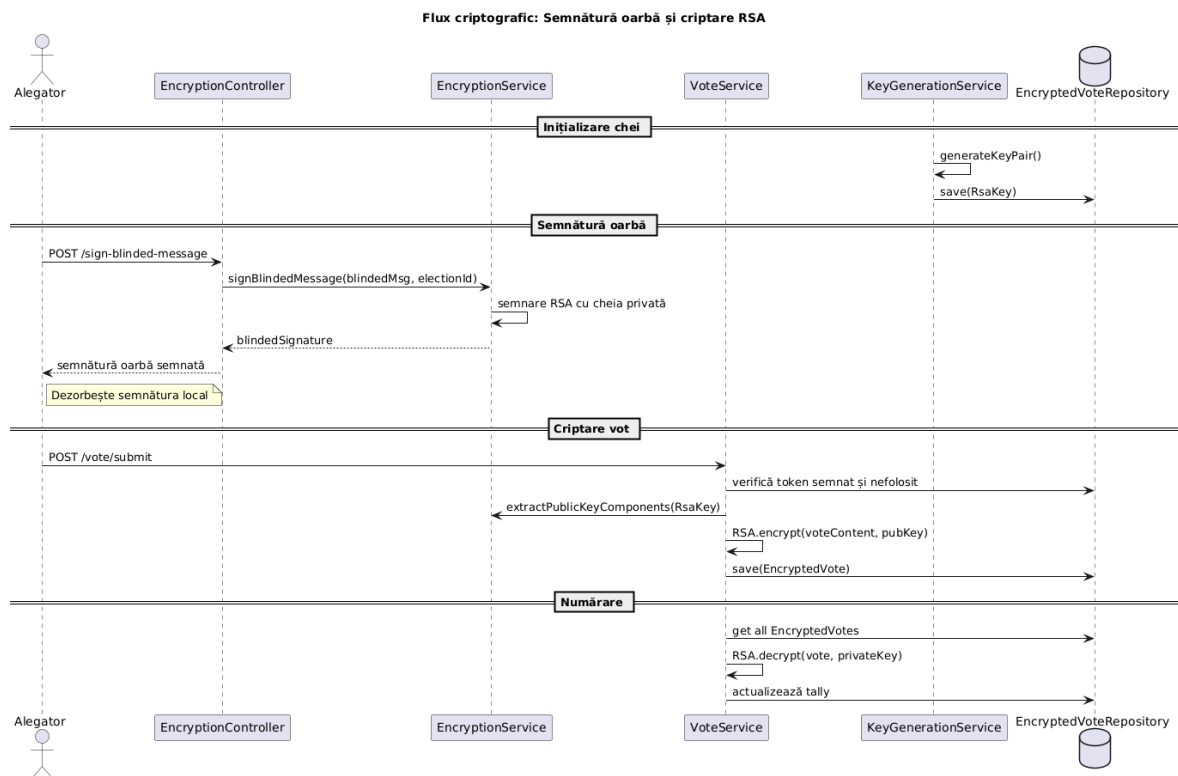


Figura 7.9: Diagramă de secvență semnătură oarbă și criptare RSA în aplicație

Capitolul 8

Măsuri de securitate în sistemul de vot

Securitatea este o componentă esențială a oricărui sistem de vot electronic, afectând direct încrederea alegătorilor și legitimitatea rezultatului. Sistemul propus integrează măsuri tehnice care vizează protejarea confidențialității, prevenirea fraudei și asigurarea integrității datelor, folosind mecanisme criptografice moderne și o arhitectură separată logic pe componente.

8.1 Modelul de securitate aplicat

Arhitectura sistemului reflectă principii consacrate din securitatea informației: confidențialitate, integritate, disponibilitate și verificabilitate. Aceste principii sunt implementate prin:

- utilizarea criptografiei RSA pentru criptarea voturilor;
- mecanismul de semnătură oarbă asupra tokenurilor anonime;
- separarea logică între identitatea alegătorului și buletinul de vot;
- validarea strictă a tokenurilor anonime la fiecare pas;
- marcarea permanentă a tokenurilor folosite pentru a preveni votul multiplu.

8.2 Izolarea identității alegătorului

Sistemul separă complet procesul de autentificare de procesul de vot. Alegătorul se autentifică pentru a primi un token anonim, care este semnat în orb de autoritatea electorală, fără ca aceasta să cunoască conținutul semnat. Tokenul astfel semnat este utilizat ulterior pentru trimiterea votului, fără a mai fi nevoie de reautentificare. În

baza de date, entitatea `Vote` nu conține nicio referință la `Voter`, iar identificatorul buletinului de vot este disociat complet de utilizator.

8.3 Prevenirea votului multiplu

Fiecare credential anonim este verificat înainte de a fi folosit pentru trimiterea unui vot. În clasa `VoteService`, sistemul validează că tokenul nu a fost deja utilizat și corespunde alegerii curente. Dacă este valid, votul este acceptat, iar tokenul este imediat marcat ca folosit:

```
matchingCredential.setUsed(true);  
blindCredentialRepository.save(matchingCredential);
```

Astfel, nicio tentativă de reutilizare a unui token nu va fi acceptată. Răspunsul standard returnat este `403 Forbidden` în caz de token invalid sau deja folosit.

8.4 Criptarea votului și integritatea datelor

Votul propriu-zis este criptat cu cheia publică RSA asociată alegerii. Clasa `VoteService` utilizează biblioteca standard Java `Cipher` pentru a cripta conținutul votului înainte de salvare:

```
cipher.init(Cipher.ENCRYPT_MODE, publicKey);  
byte[] encryptedVote = cipher.doFinal(voteContent.getBytes(  
    StandardCharsets.UTF_8));
```

Această criptare garantează că niciun vot nu poate fi citit în timpul procesului electoral. Decriptarea este permisă doar la finalul alegerii, folosind cheia privată aferentă, gestionată de autoritatea electorală.

8.5 Controlul accesului și validarea datelor

Sistemul include validări riguroase pe fiecare punct de intrare. DTO-urile folosite pentru trimiterea datelor (ex. `VoteDTO`, `BlindedMessageDTO`) sunt adnotate cu constrângeri, iar serverul respinge automat orice cerere invalidă sau malformată înainte ca aceasta să intre în fluxul de criptare.

8.6 Canalul de comunicare

În această implementare, comunicarea dintre client și server are loc prin protocol HTTP simplu, fără criptare la nivel de transport. Acest lucru înseamnă că datele

transmise pot fi interceptate sau modificate în rețele nesecurizate, reprezentând o vulnerabilitate în medii de producție.

Totuși, sistemul compensează parțial acest aspect prin măsuri criptografice aplicate la nivel de aplicație:

- voturile sunt criptate local, în backend, cu cheia publică RSA a alegerii;
- tokenurile anonime nu conțin informații identificabile și sunt valabile o singură dată;
- nu există transmisii directe de date personale în timpul procesului de vot.

Capitolul 9

Importanța sociologică a votului într-o societate democratică

9.1 Votul ca fundament al democrației

Votul este unul dintre pilonii centrali ai democrației moderne. Prin intermediul votului, cetățenii participă la viața politică, își exprimă voința și contribuie la conturarea direcției în care se îndreaptă societatea. Fără vot, legitimitatea structurilor politice ar fi fragilă, iar controlul democratic asupra puterii ar deveni iluzoriu. Așa cum afirmă Lipset și Rokkan, structurile de clivaj social influențează nu doar aliniamentele partidelor, ci și participarea electorală în sine [LR67].

9.2 Dimensiunea socială și identitară a votului

Actul de a vota nu este doar o decizie politică, ci și una cu puternice implicații sociale. Alegerea unui candidat sau a unei politici reflectă identitatea socială, apartenența de grup, experiențele personale și valorile indivizilor. Conform teoriei sociologice columbiene (Columbia School), comportamentul electoral este adesea determinat de factori de grup precum religia, clasa socială și mediul familial [LBG54].

Votul funcționează astfel ca un mecanism de validare identitară și de afiliere la o comunitate imaginată a „cetățenilor activi”.

9.3 Consecințele absenteismului și ale neîncrederii

O prezență scăzută la vot reflectă adesea neîncrederea în instituțiile statului și poate duce la dezechilibre de reprezentare. Grupurile vulnerabile sau marginalizate riscă să rămână fără voce în deciziile publice. În mod ironic, exact cei care ar avea cel mai mult de câștigat din participare sunt cei mai puțin prezenți la urne.

Potrivit lui Russell Dalton și Martin Wattenberg, actul de a vota este „departe de a fi un gest simplu” – este influențat de factori psihologici, socioeconomi și instituționali [DW00].

9.4 Capitalul social și implicarea civică

Robert Putnam, în lucrarea sa despre capitalul social, subliniază faptul că participarea electorală este o expresie a sănătății civice a unei societăți. O rată mare de participare la vot este corelată cu alte forme de implicare socială – voluntariat, încredere în semenii, coeziune comunitară. Pe de altă parte, o scădere a participării indică izolarea individului față de sistemul politic [Put00].

9.5 Considerații legale și etice

Deși această lucrare se concentrează asupra aspectelor tehnice ale votului electronic, este esențială și analiza implicațiilor legale și etice, întrucât orice sistem de vot trebuie să respecte principii democratice fundamentale, legislația în vigoare și normele de protecție a datelor.

În România, cadrul legislativ actual nu reglementează explicit votul electronic la scară națională. Codul electoral (Legea nr. 208/2015) nu conține prevederi referitoare la votul prin internet, dar permite desfășurarea de proiecte pilot, cu aprobarea Autorității Electorale Permanente (AEP). În schimb, la nivel european, există o serie de recomandări formulate de organisme internaționale precum Consiliul Europei, OSCE sau Comisia de la Veneția, care subliniază importanța transparenței și respectării drepturilor electorale [Eur04; OSC13].

Din perspectivă etică, votul electronic aduce provocări particulare, precum riscul de coerciție sau excluderea digitală. De asemenea, conformitatea cu Regulamentul General privind Protecția Datelor (GDPR) este esențială pentru un sistem responsabil, în special atunci când sunt prelucrate date sensibile cum ar fi CNP-ul, adresa sau imaginea de profil a alegătorului.

9.6 Rolul votului electronic în extinderea participării

Votul electronic promite să elimine unele bariere tradiționale: distanța, timpul, mobilitatea redusă. Astfel, anumite grupuri – diaspora, persoanele cu dizabilități, studenții – pot deveni mai active în viața democratică. Studiile arată că în țări care au adoptat e-voting pentru alegeri locale sau consultări, participarea a crescut [OSC13].

Totuși, votul electronic aduce și noi provocări sociologice:

- **Excluziunea digitală** – lipsa alfabetizării digitale sau a accesului la tehnologie poate marginaliza anumite categorii sociale [Put00];
- **Neîncrederea în tehnologie** – lipsa transparenței sau lipsa înțelegerii mecanismelor criptografice poate reduce încrederea [MH11];
- **Percepția asupra anonimatului** – dacă sistemele nu sunt bine explicate publicului, votanții pot evita participarea de teamă că votul lor nu este secret.

9.7 Votul și responsabilitatea civică

Participarea la vot nu este doar un drept, ci și o responsabilitate democratică. Prin vot, cetățenii își asumă rolul de supraveghetori ai puterii. Un sistem democratic sustenabil necesită implicarea continuă a cetățenilor, nu doar prin vot, ci și prin monitorizare, protest, dialog și educație civică.

Sociologii subliniază importanța internalizării acestei responsabilități încă din educația timpurie [Put00].

9.8 Acceptabilitatea votului electronic în România

9.8.1 Studiile internaționale și europene

Potrivit unui sondaj Eurobarometru (2023), doar 38% dintre respondenții din România au declarat că ar avea încredere mare sau foarte mare în votul prin internet, comparativ cu o medie de 51% la nivelul Uniunii Europene [Com23].

Într-un raport al OSCE/ODIHR, se remarcă faptul că România nu a implementat un sistem de vot electronic din cauza lipsei consensului politic și a îngrijorărilor legate de securitate [OSC13].

9.8.2 Atitudinea alegătorilor români

MIT Election Data and Science Lab arată că sprijinul pentru votul online este semnificativ mai mare în rândul românilor din diaspora (peste 60%), în comparație cu cetățenii rezidenți în țară (sub 40%) [Ope19].

Datele INSCOP confirmă aceste tendințe: 44% dintre români consideră că votul electronic ar reduce fraudă, 31% cred că ar crește participarea tinerilor, iar 49% se tem că votul lor nu ar rămâne secret [INS22].

România nu este încă pregătită pentru o adoptare completă a votului online, dar direcția este deschisă pentru testare graduală și integrare în etape, în special în contextul tehnologic în evoluție și al nevoii de modernizare democratică.

Capitolul 10

Concluzii

Lucrarea de față și-a propus proiectarea și realizarea unui sistem electronic de vot anonim, care să răspundă cerințelor moderne de securitate, transparență și accesibilitate. Pornind de la o bază teoretică solidă, au fost analizate conceptele esențiale ale votului electronic, precum anonimitatea, integritatea datelor, criptografia asimetrică și protocoalele de semnătură oarbă.

Contribuția originală constă nu doar în integrarea acestor tehnologii, ci și în implementarea unui sistem coerent care simulează fidel procesele unui scrutin real. Totodată, capitolul final al lucrării a oferit o perspectivă cantitativă și teoretică asupra puterii de vot și a modului în care aceasta poate fi modelată matematic, deschizând oportunități pentru extinderea funcționalităților sistemului în direcția alegerilor delegate, votului ponderat sau simulărilor electorale avansate.

Limitările actuale se referă la lipsa unei verificabilități universale, a dovezilor criptografice de tip *Zero-Knowledge* și a unei infrastructuri de audit extern complet. De asemenea, protocolul de comunicație nu utilizează încă HTTPS, dar arhitectura modulară permite adăugarea acestor componente într-un mod transparent și scalabil.

Perspective de dezvoltare viitoare includ:

- integrarea unui modul de audit extern și loguri criptografice;
- folosirea dovezilor ZKP pentru creșterea încrederii în sistem;
- suport pentru votul prin mobil și extensii biometrice;
- introducerea unui AI pentru detectarea anomaliilor și recomandări electorale;
- exportul de rezultate și jurnale în formate standardizate.

În concluzie, lucrarea demonstrează fezabilitatea și potențialul unui sistem electronic de vot construit pe principii solide de securitate și confidențialitate. Deși încă nu este pregătit pentru alegeri la scară națională, sistemul implementat oferă o bază solidă pentru cercetare și dezvoltare viitoare în domeniul *e-voting*-ului sigur și transparent.

Bibliografie

- [Adi08] Ben Adida, *Helios Voting System*, https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf, 2008.
- [AT02] Jonathan N. Katz Andrew Gelman și Francis Tuerlinckx, *The Mathematics and Statistics of Voting Power*, 2002, URL: <https://sites.stat.columbia.edu/gelman/research/published/STS027.pdf>.
- [Ben06] Josh Benaloh, “Verifiable secret-ballot elections”, în 2006, URL: <https://www.cs.yale.edu/publications/techreports/tr561.pdf>.
- [Bra07] Steven J. Brams, “Mathematics and Democracy: Designing Better Voting and Fair-Division Procedures”, în *The College Mathematics Journal* (2007), URL: <https://ww2.amstat.org/mam/08/BramsMathematicsandDemocracy.pdf>.
- [Cha81] David Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, 1981, URL: <https://doi.org/10.1145/358549.358563>.
- [Cha82] David Chaum, *Blind Signatures for Untraceable Payments*, 1982, URL: <https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF>.
- [Com23] Comisia Europeană, *Eurobarometru Standard 99: Percepția cetățenilor asupra democrației în UE*, <https://europa.eu/eurobarometer>, 2023.
- [DH76] Whitfield Diffie și Martin Hellman, “New directions in cryptography”, în *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654, DOI: <https://ieeexplore.ieee.org/document/1055638>.
- [DW00] Russell J. Dalton și Martin P. Wattenberg, *Democracy Transformed: Expanding Political Opportunities in Advanced Industrial Democracies*, Oxford University Press, 2000, URL: <https://pdfroom.com/books/democracy-transformed-expanding-political-opportunities-in-advanced-industrial-democracies-comparative-politics-oxford-university-press/j9ZdYw0E2V4>.

- [Est17] State Electoral Service of Estonia, *Estonia's Internet Voting System Framework*, <https://www.regeringen.ax/sites/default/files/attachments/page/estonia-e-voting-2017.pdf>, 2017.
- [Eur04] Council of Europe, *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*, 2004, URL: [https://www.coe.int/t/dgap/goodgovernance/activities/key-texts/recommendations/00Rec\(2004\)11_rec_adopted_en.asp](https://www.coe.int/t/dgap/goodgovernance/activities/key-texts/recommendations/00Rec(2004)11_rec_adopted_en.asp).
- [FM01] Josep Freixas și Dominik Marciniak, “Weighted Voting Systems and Applications in Game Theory”, în *Mathematics and Computers in Simulation* 56 (2001), pp. 119–129.
- [Gal08] Serge Galam, “Sociophysics: A Review of Galam Models”, în (2008), URL: <https://arxiv.org/pdf/0803.1800>.
- [Gel+08] Andrew Gelman et al., *Red State, Blue State, Rich State, Poor State: Why Americans Vote the Way They Do*, Princeton University Press, 2008, URL: https://www.researchgate.net/publication/289976344_Red_state_blue_state_rich_state_poor_state_Why_Americans_vote_the_way_they_do_Expanded_edition.
- [GH04] Andrew Gelman și Jennifer Hill, “Average predictive comparisons for models with nonlinearity, interactions, and variance components”, în *Sociological Methodology* (2004), URL: <https://sites.stat.columbia.edu/gelman/research/published/ape17.pdf>.
- [GH07] Andrew Gelman și Jennifer Hill, “Data Analysis Using Regression and Multilevel/Hierarchical Models”, în *Cambridge University Press* (2007), URL: <https://scispace.com/pdf/data-analysis-using-regression-and-multilevel-hierarchical-31gve8l12s.pdf>.
- [Gri03] Dimitris Gritzalis, *Secure Electronic Voting*, 2003, URL: <https://www.infosec.aueb.gr/Publications/CSIRT-2003.pdf>.
- [INS22] INSCOP Research, *Barometrul de Opinie Publică – Votul electronic în România*, <https://democracycenter.ro/publicatii/cat-de-oportuna-este-introducerea-votului-prin-internet-romania/>, 2022.
- [Joh06] Erik Johansson, “Implementing Mix-Nets for Universal Verifiability in Electronic Voting”, Teză de dizert., Umeå University, Sweden, 2006, URL: <https://www.diva-portal.org/smash/get/diva2:703604/FULLTEXT02>.

-
- [LBG54] Paul F. Lazarsfeld, Bernard Berelson și Hazel Gaudet, *The People's Choice: How the Voter Makes Up His Mind in a Presidential Campaign*, Columbia University Press, 1954, URL: <https://dokumen.pub/the-peoples-choice-how-the-voter-makes-up-his-mind-in-a-presidential-campaign-9780231896146.html>.
- [LR67] Seymour M. Lipset și Stein Rokkan, *Party Systems and Voter Alignments: Cross-National Perspectives*, New York: Free Press, 1967, URL: https://www.researchgate.net/publication/323029695_Party_Systems_and_Voter_Alignments.
- [MH11] Sofie Marien și Marc Hooghe, “Does Political Trust Matter? An Empirical Investigation into the Relation Between Political Trust and Support for Law Compliance”, în *European Journal of Political Research* (2011), URL: <https://discovery.researcher.life/article/does-political-trust-matter-an-empirical-investigation-into-the-relation-between-political-trust-and-support-for-law-compliance/92b392f55cae3e58ab>
- [MKJ16] K. Moriarty, B. Kaliski și J. Jonsson, *PKCS #1: RSA Cryptography Specifications Version 2.2*, RFC 8017, 2016, URL: <https://www.rfc-editor.org/info/rfc8017>.
- [MOV96] Alfred J. Menezes, Paul C. van Oorschot și Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996, URL: <https://cacr.uwaterloo.ca/hac/>.
- [Nat19] National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, rap. teh. NIST SP 800-56B Revision 2, U.S. Department of Commerce, 2019, URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf>.
- [Ope19] Rand Europe Open Evidence, *Study on the benefits and drawbacks of remote voting solutions to support the preparation of a best practice guide for the use of digital tools to facilitate the exercise of EU citizens' political rights*, https://commission.europa.eu/system/files/2019-11/remote_voting_main_findings.pdf, 2019.
- [OSC13] OSCE, *Handbook For the Observation of New Voting Technologies*, Office for Democratic Institutions și Human Rights, 2013, URL: <https://www.osce.org/files/f/documents/0/6/104939.pdf>.
- [Pen46] Lionel S. Penrose, *The Elementary Statistics of Majority Voting*, vol. 109, 1, 1946, URL: <https://academic.oup.com/jrsssa/article/109/1/53/7097074>.
-

- [Put00] Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community*, Simon & Schuster, 2000, URL: <https://communistcaucus.com/wp-content/uploads/2021/12/Bowling-Alone.pdf>.
- [Riv06] Ronald L. Rivest, “Electronic voting: the devil is in the details”, în *Proceedings of the 2006 Electronic Voting Technology Workshop (EVT)*, 2006, URL: <https://people.csail.mit.edu/rivest/pubs.html>.
- [RSA78] Ronald L. Rivest, Adi Shamir și Leonard Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, în *Communications of the ACM* 21.2 (1978), pp. 120–126, DOI: 10.1145/359340.359342, URL: <https://people.csail.mit.edu/rivest/Rsapaper.pdf>.
- [SB23] Ben Smyth și Fabrice Benhamouda, *Blind RSA Signatures*, rap. teh. RFC 9474, RFC Editor, 2023, URL: <https://www.rfc-editor.org/info/rfc9474>.
- [SR21] A. Shrestha și S. Rizvi, *REVS – A Robust Electronic Voting System*, 2021, URL: <https://ieeexplore.ieee.org/document/9473813>.
- [Sta11] William Stallings, *Cryptography and Network Security: Principles and Practice*, a 5-a ed., 2011, URL: https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf.