ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Dipartimento di Informatica — Scienza e Ingegneria (DISI)

Corso di Laurea in Ingegneria e Scienze Informatiche

Applicazione della Crittografia nei Sistemi di Voto Digitale

Tesi di laurea

Relatore
Prof. Luciano Margara

Presentata da
Giorgia Patera

Sessione: Marzo 2026
Anno Accademico 2025/2026

Sommario

La presente tesi esplora i sistemi di voto elettronico con particolare attenzione agli aspetti crittografici, tecnologici e normativi. L'obiettivo è fornire una panoramica completa dei requisiti di sicurezza e affidabilità necessari per garantire che il voto digitale sia sicuro, verificabile e rispettoso dei principi democratici. Il lavoro è organizzato in più capitoli. Nel Capitolo 2 vengono analizzati i requisiti fondamentali di un sistema di voto digitale, come l'idoneità al voto (eligibility), la verificabilità dell'elettore e universale, la non dimostrabilità del voto (receipt-freeness) e la resistenza alla coercizione. Questi principi costituiscono la base per la progettazione di sistemi affidabili. Il Capitolo 3 approfondisce i fondamenti crittografici che rendono possibili i sistemi di voto elettronico sicuri. Si discutono la crittografia asimmetrica (RSA, ElGamal), la crittografia omomorfica, le firme digitali, gli schemi di commitment e le prove a conoscenza zero (Zero-Knowledge Proofs), spiegando come ciascuna tecnica contribuisca a garantire sicurezza, privacy e verificabilità dei voti. Il Capitolo 4 introduce i principali paradigmi di sistemi di voto elettronico, tra cui mix-nets, sistemi omomorfici, soluzioni End-to-End Verifiable (E2E) e sistemi basati su blockchain. Vengono illustrati vantaggi e limitazioni di ciascun approccio, con esempi di implementazioni reali. Nel Capitolo 5 vengono analizzati esempi concreti di sistemi crittografici adottati in vari paesi, come Estonia, Svizzera, Brasile e Stati Uniti, evidenziando somiglianze, differenze e criticità operative. Successivamente, il Capitolo 6 approfondisce alcuni casi studio significativi, tra cui Helios, Prêt à Voter, Scantegrity e Punchscan, mostrando applicazioni pratiche dei paradigmi teorici. Il Capitolo 7 e l'8 affrontano rispettivamente la sicurezza del client votante e dei dispositivi elettorali e le problematiche legate all'usabilità e al fattore umano, sottolineando come la tecnologia debba essere progettata anche considerando l'esperienza dell'elettore. Il Capitolo 9 propone una simulazione di attacco a un sistema di voto crittografico semplificato, illustrando i rischi concreti e le possibili contromisure. Il Capitolo 10 mette a confronto i diversi sistemi analizzati, evidenziando punti di forza e limiti. Infine, il Capitolo 11 descrive gli aspetti pratici e normativi. Il Capitolo 12 conclude la tesi sottolineando come la combinazione di sicurezza crittografica, normative adeguate e fiducia pubblica sia essenziale per l'adozione diffusa del voto elettronico. Questa tesi fornisce dunque una visione completa e integrata del voto elettronico sicuro, combinando teoria, applicazioni pratiche e riferimenti normativi, utile sia per ricercatori che per professionisti interessati al tema.

Indice

1 Introduzione

L'enorme evoluzione avvenuta negli ultimi anni nell'ambito delle tecnologie, ha trasformato il modo in cui le persone, in particolare cittadini, le istituzioni e le imprese, iteragiscono tra loro. In particolare nell'ambito dei servizi pubblici, grazie alla digitalizzazione c'è stata la possibilità di migliorare la trasparenza e l'efficienza dei servizi. Un servizio pubblico molto discusso in questo momento e capiremo successivamente il motivo è il voto elettronico. Esso è una delle sfide più delicate e controverse, perchè da un lato offre l'opportunità di ridurre i costi organizzativi e aumentare la partecipazione al voto, non avendo l'obbligo di recarsi fisicamente nelle urne elettorali, può essere molto più comodo per giovani che vivono per motivi lavorativi o di studio lontani dalla residenza ma anche per persone anziane o con difficoltà a spostarsi. Però, dall'altro lato, introduce rischi tecnici e giuridici che possono compromettere la democrazia e la veridicità del voto che impongono un'analisi attenta.

Il processo di voto è una procedura di per se molto complicata che richiede come sappiamo un equilibrio complesso tra anonimato, integrità, autenticità e verificabilità. Il sistema di voto, a differenza di tutti gli altri sistemi digitali, infatti, non deve soltanto proteggere i dati degli utenti, ma deve garantire che ogni voto sia registrato correttamente, che nessun elettore possa votare più di una volta e, allo stesso tempo, che il voto resti segreto. Una serie di requisiti spesso difficili da rispettare in contemporanea, ma che rendono il voto elettronico un ambito di studio unico e particolarmente complesso.

Grazie alla crittografia moderna riusciamo oggi a realizzare sistemi di voto sicuri. Con l'utilizzo di alcune tecniche, che spiegherò in seguito, come la crittografia asimmetrica, le firme digitali, le blid signature, i meccanismi di commitment e le zero-knowledge proofs si riescono a realizzare protocolli in grado di conciliare segretezza e verificabilità. A queste tecniche si aggiungono anche approcci più avanzati, come la crittografia omomorfica e le mix-nets, che consentono di elaborare o anonimizzare i voti senza rivelarne il contenuto, anche queste verranno esposte in seguito. All'interno di questo elaborato vedremo anche come negli ultimi vent'anni e tutt'ora diversi paesi hanno sperimentato forme di voto elettronico, con risultati diversi. Per esempio l'Estonia ha implementato un modello nazionale basato su carte d'identità digitali, la Svizzera invece ha testato sistemi crittografici complessi come Swiss Post. Tutto questo perchè queste esperienze possano offrire un panorama ricco e utile per comprendere punti di forza, limiti e insegnamenti da cui imparare.

All'interno di questa tesi ho come obiettivo analizzare in profondità come la crittografia venga applicata nei sistemi di voto digitale, da due punti di vista, da un lato chiarire quali meccanismi è possibile utilizzare perchè garantiscono i requisiti fondamentali di un'elezione democratica. Dall'altro lato valutare attraverso casi reali e simulazioni, quali sono i rischi che comunque rimangono anche utilizzando tecniche avanzate. Verranno illustrati

particolarmente i sistemi end-to-end verifiable, considerati oggi tra i più promettenti, e osserveremo anche le problematiche relative al dispositivo dell'elettore, che spesso viene trascurato ma cruciale per un voto sicuro. Successivamente metterò in comparazione i vari modelli proposti evidenzando vantaggi, limiti e le condizioni necessarie per poterli applicare in modo affidabile. L'obiettivo finale è comprendere cosa serve per rendere il voto digitale sicuro, affidabile e compatibile con i principi fondamentali di una società democratica ma anche comprende quanto è fondamentale e ovunque la crittografia al giorno d'oggi, apprezzandone la complessità e le numerose opportunità che è ancora in grado di offrire.

2 Requisiti di un sistema di voto digitale

Un sistema di voto elettronico esattamente come l'elezioni tradizionali, deve avere e rispettare dei requisiti fondamentali, che sono alla base di una democrazia. A differenza degli altri sistemi informatici, all'interno del voto digitale questi requisiti devono coesistere. Il protocollo crittografico per il voto si fonda quindi sulla capacità di conciliare sicurezza, trasparenza, verificabilità e tutela della libertà dell'elettore.

Questo capitolo approfondisce i principali requisiti riconosciuti internazionalmente nel sistema di voto:

- Eligibility - (Idoneità al voto)
- Voter verifiability - (Verificabilità dell'elettore)
- Universal verifiability - (Verificabilità universale)
- Receipt-freeness - (Non dimostrabilità del voto)
- Coercion resistance - (Resistenza alla coercizione)

Ognuno di essi rappresenta una condizione necessaria affinchè un'elezione possa essere considerata affidabile, trasparente e conforme ai principi democratici. Tutti questi requisiti sono considerati cruciali nella progettazione dei sistemi di voto elettronico [Int26].

2.1 Eligibility - (Idoneità al voto)

Il primo requisito è assicurare che solo chi ne ha diritto può votare, e possa votare una e una sola volta. Nei sistemi tradizionali, ovvero nelle urne elettorali, applicare questo principio è molto semplice, attraverso i registri elettorali e un documento valido, si identifica fisicamente la persona e controllando i seggi si fa si che la persona voti una sola volta. In un sistema digitale, invece, è leggermente più complicato, l'autenticazione avviene tramite credenziali elettroniche, certificati digitali o dispositivi crittografici personali.

I problemi, però, possono essere svariati; innanzitutto, il sistema deve riconoscere l'elettore per impedirne l'impersonificazione e la sostituzione di persona, ma non bisogna collegare tale identità al contenuto del voto, per mantenere l'anonimato del voto e preservare la segretezza. Questo problema la crittografia cerca di risolverlo attraverso meccanismi come firme anonime, blind signature e l'uso di chiavi diverse per autenticazione e cifratura.

Le blind signature, che vedremo in maniera approfondita successivamente, permettono a un'autorità di certificare che l'elettore abbia il diritto a votare, senza però conoscere il contenuto del voto: l'elettore "offusca" il voto prima della firma e poi lo invia cifrato. In questo modo si mantiene l'anonimato. In molti sistemi digitali, invece si utilizzano chiavi separate per autenticazione e per la cifratura del voto. L'elettore si autentica con la propria chiave privata per dimostrare il diritto al voto, mentre il voto viene cifrato con una chiave diversa, rendendo impossibile associare identità e scelta. Vedremo in maniera approfondita le tecniche come blid-signature e molte altre che permettono alla crittografia di attuare questo principio anche nel voto elettronico.

2.2 Voter verifiability - (Verificabilità dell'elettore)

La verificabilità dell'elettore consiste nel fatto che esso possa controllare che il proprio voto sia stato registrato e conteggiato correttamente, senza dover rivelare il contenuto a terzi. In pratica ogni elettore deve poter verificare che il suo voto sia stato accettato dal sistema, che esso conservi l'integrità lungo tutta la catena di elaborazione e che la registrazione effettuata sia realmente quella che lui ha espresso.

A differenza dell'urna cartacea, dove la fiducia è delegata alle procedure dei seggi, nel voto digitale questa garanzia deve essere fornita in modo matematico e verificabile. Un sistema che rispetta questo requisito fornisce all'elettore una forma di prova o codice di conferma che consente di verificare che il proprio voto è stato ricevuto, non sia stato alterato e sia effettivamente presente nello scrutino. Per realizzare questa proprietà vengono utilizzate diverse tecniche tra cui, per esempio ricevute crittografiche, che non rivelano la scelta politica ma permettono di ritrovare il voto. Un esempio concreto è il sistema Helios, che permette a un elettore di verificare tramite una pagina pubblica che il suo voto sia stato incluso nel conteggio, senza doverlo rivelare. [Hel26].

Questo requisito è essenziale perchè aumentando la trasparenza all'interno del processo elettorale, si riduce la fiducia cieca nella gestione del sistema.

2.3 Universal verifiability - (Verificabilità universale)

La verificabilità universale consiste nella possibilità per chiunque di controllare, non solo come singolo elettore, ma come collettività, ovvero chiunque, anche senza aver votato, deve poter verificare che il conteggio finale dei voti sia corretto e completo. Nel voto

elettronico questo parametro è fondamentale perchè gran parte del processo non è visibile fisicamente, e l'ente che gestisce le elezioni non deve essere l'unico a garantire la correttezza dei risultati.

Per raggiungere questa proprietà un sistema deve pubblicare le prove crittografiche del conteggio e rendere disponibili i dati crittografici dei voti. Naturalmente ciò deve avvenire senza compromettere la segretezza dei voti dei singoli elettori. I sistemi end-to-end per esempio sono nati proprio per questo motivo: permettono a qualsiasi soggetto competente come ricercatore o ente di controllo o anche semplice cittadino, di ricostruire lo scrutinio verificandone la correttezza dall'esterno. Anche i sistemi basati su mix-nets o su crittografia omomorfica sono particolarmente adatti a questo scopo perchè permettono di verificare che le operazioni crittografiche siano corrette e offrono prove pubbliche della correttezza del conteggio.

L'universal verifiability è considerata una delle proprietà che differenziano maggiormente un sistema di voto elettronico maturo da sistemi più semplici.

2.4 Receipt-freeness - (Non dimostrabilità del voto)

La receipt-freeness riguarda la capacità del sistema di impedire all'elettore di ottenere una prova con cui dimostrare a una terza persona chi ha votato, ovvero la preferenza espressa. [MBC26].

Senza la presenza di questo requisito sarebbero possibili la compravendita di voto, il controllo dell'elettore da parte di organizzazioni, oppure semplicemente pressioni familiari o politiche. Ovviamente questa proprietà esiste anche nel voto cartaceo, l'elettore quando entra nel seggio e vota non deve produrre nessuna prova della sua scelta. Ma nel voto elettronico il rischio è maggiore perchè la ricevuta restituita dal sistema può essere utilizzata come prova o l'interfaccia utente può essere fotografata, ci sono un'enorme quantità di possibilità in cui l'elettore può avere una prova della sua preferenza avendo meno controllo effettivo. Per cercare di risolvere questo problema si usano soluzioni come ricevute crittografiche non dimostrabili, voti randomizzati, dove due voti identici possono risultare crittograficamente diversi, o meccanismi di "contestazione", in cui l'elettore può invalidare la propria ricevuta rendendola inutilizzabile.

Il giusto equilibrio tra l'impedire abusi e rendere il voto sicuro e libero da qualsiasi tipo di interferenze, sia economiche che sociali, è molto importante.

2.5 Coercion resistance - (Resistenza alla coercizione)

La coercione della resistenza è come la receipt-freeness, ma in una forma più estesa e più forte. In pratica, il problema non è solo evitare che l'elettore possa fornire volontariamente una prova del proprio voto, ma proteggere l'elettore anche nel caso in cui sia sotto coercizione attiva o sorvegliata. Per esempio, l'elettore vota da casa con un coercitore

presente, o l'elettore è sotto minaccia che impone di votare in un determinato modo, o addirittura un voto effettuato da terzi utilizzando le credenziali dell'elettore.

Per garantire questo requisito nel sistema devono essere possibili, per esempio voti falsi o "di copertura", dove l'elettore può fingere di votare in un determinato modo ma il voto reale rimane segreto. Per esempio inserire la possibilità di rivotare, in modo che il coercitore non può sapere se il voto finale è quello che pensa, meccanismi per cui non esistano dati dimostrativi del voto reale, e soprattutto separare l'autenticazione dalla generazione del voto, impedendo il correlamento tra persona e voto [Cha+24].

Nonostante queste svariate soluzioni questo requisito rimane uno dei più complessi da realizzare in pratica e la principale criticità nei sistemi di voto, uno dei principali motivi per cui molti paesi limitano o addirittura vietano il voto online domestico.

2.6 Considerazioni finali

Per ottenere un sistema di voto elettronico che rispetta i principi della democrazia, bisogna riuscire a realizzare e implementare tutti questi requisiti contemporaneamente, non sempre è facile perchè il raggiungimento di una proprietà potrebbe rende più difficile ottenerne e realizzarne un'altra. Per esempio maggiore verificabilità può andare in contrasto e rischia di ridurre la segretezza, o maggiore anonimato può rendere più complesso evitare i dati multipli o addirittura la protezione contro la coercizione può ridurre la trasparenza immediata. Per questo motivo, la crittografia moderna è diventata essenziale nel voto digitale, perchè introduce garanzie matematiche e prove verificabili in modo pubblico, aumentando la fiducia nell'autorità elettorale.

Infine nonostante le criticità è importante riuscire a realizzare in contemporanea i requisiti, ottenendo un equilibrio tra essi, per produrre un sistema di voto elettronico affidabile, sicuro e trasparente.

3 Fondamenti crittografici nei sistemi di voto elettronico

La realizzazione di un sistema di voto elettronico affidabile non dipende da una buona struttura informatica, ma come abbiamo visto a lezione, è molto più importante l'utilizzo di tecniche crittografiche capaci di rispettare i requisiti visti nel capitolo precedente, che sono estremamente difficili da garantire simultaneamente. Come abbiamo affermato precedentemente, il sistema deve sapere chi sta votando, ma non che cosa sta votando, mentre al contrario gli osservatori devono poter verificare che il risultato finale sia corretto senza poter accedere ai voti individuali. La soluzione a questo paradosso è di natura matematica, grazie alla crittografia moderna che si basa su fondamenti matematici abbiamo degli strumenti specifici che ci permettono di dividere e isolare le varie fasi del

processo elettorale in modo tale da non tradire nessun requisito e riuscire a realizzarli tutti contemporaneamente.

Tra i vari strumenti della crittografia moderna i più utilizzati e che vedremo in questo capitolo sono: la crittografia asimmetrica, la crittografia omomorfica, le firme digitali e blind signature, commitment scheme, infine prove a conoscenza zero (zero-knowledge proofs). Nei paragrafi seguenti spiegherò brevemente cosa sono questi strumenti e come vengono utilizzati, soprattutto nell'ambito del voto elettronico.

3.1 Crittografia Asimmetrica (RSA, ElGamal)

Esistono due grandi categorie, la crittografia asimmetrica e la crittografia simmetrica. La crittografia simmetrica utilizza una singola chiave che viene condivisa in segreto tra chi cifra e chi decifra. La crittografia asimetrica invece utilizza due chiave diverse ma matematicamente correlate: una chiave pubblica, diffusa e nota a tutti e una chiave privata che invece è segreta e solo di chi riceve il messaggio. La crittografia asimmetrica si basa sul principio che chiunque può cifrare un messaggio con la chiave pubblica, ma solo chi possiede la chiave privata può decifrarlo. Al giorno d'oggi la crittografia asimmetrica è la base della maggior parte dei sistemi di voto elettronici e non solo. [Nor24]

Nel voto, questo meccanismo è fondamentale perchè consente di cifrare la scheda elettorale in modo che solo l'ente autorizzato possa leggerla e permette di separare la fase di autenticazione dell'elettore dalla fase di espressione del voto. Inoltre la chiave pubblica è uguale per tutti gli elettori, garantendo uniformità e trasparenza nel trattamento dei voti. Un'altra cosa importante è che chi vota può identificarsi, con un certificato digitale o con una chiave personale, ma il voto viene coperto con un codice, facendo ciò impedisce all'autorità elettorale di associare le due informazioni.

La crittografia asimmetrica si basa su problemi matematici molto difficili da risolvere. Per esempio, un problema è prendere un numero molto grande e trovare da quali numeri più piccoli si ottiene, ovvero la fattorizzazione. Un altro problema usato si chiama logaritmo discreto, che si intende trovare un numero nascosto quando si conoscono solo i risultati di calcoli in gruppi particolari. Questi problemi sono molto lenti da risolvere con i metodi di calcolo normali, mentre le operazioni per cifrare e decifrare sono più facili e rapide. Gli algoritmi più conosciuti che usano queste idee sono RSA ed ElGamal. Questi vengono usati oggi per fare cose molto importanti come protocolli di autenticazione digitale, scambi sicuri con chiavi pubbliche, creare certificati elettronici e sistemi per il voto digitale. Così la crittografia rende sicuri i dati e mantiene la privacy delle persone. [IBM25a]

L'algoritmo più noto e più utilizzato all'interno della crittografia asimmetrica è RSA. E' stato creato nel 1977 da Rivest, Shamin e Adleman, si basa sulla difficoltà di dividere

un numero molto grande in fattori primi. Il funzionamento dell'algoritmo RSA può essere descritto in pochi passaggi matematici fondamentali: [Min25b]

1. Sceglie due numeri primi molto grandi p e q.
2. Calcola il modulo $n = p \cdot q$ e la funzione di Eulero $\varphi(n) = (p-1)(q-1)$.
3. Sceglie un intero e tale che $1 < e < \varphi(n)$ e $\gcd(e, \varphi(n)) = 1$.
4. Calcola un numero intero d tale che, moltiplicato per e, restituisca 1:

$$d \cdot e \equiv 1.$$

5. Ora è possibile rendere di dominio pubblico la chiave $\mathrm{K_{pub}} = (e, n)$ e tenere nascosta la chiave $\mathrm{K_{prv}} = (d, n)$.

Ogni messaggio viene rappresentato come una sequenza binaria, che viene trattata come un numero intero m. Per utilizzare RSA, deve valere:

$$m < n$$

dove n è il modulo della chiave RSA. Se il messaggio è più lungo, esso viene suddiviso in blocchi di al massimo $\lfloor \log_2(n) \rfloor$ bit.

- **Cifratura:** Il mittente cifra con la chiave pubblica il messaggio (n, e):

$$c = m^e \mod n$$

- **Decifratura:** il destinatario riceve il pacchetto cifrato. Successivamente per ottenere il messaggio originale lo cifra utilizzando la chiave privata (n, d):

$$m = c^d \mod n$$

In questo modo, anche viene intercettato il messaggio cifrato, c, non è possibile risalire al messaggio originale senza conoscere la chiave privata d.

Un messaggio che viene criptato con la chiave pubblica può essere letto solo se si utilizza la sua chiave privata, serve per dare segretezza e sicurezza. Si può anche fare il contrario, cioè criptare il messaggio con la chiave privata, così chiunque potrà leggerlo usando la sua chiave pubblica, questo meccanismo viene utilizzato per firmare i messaggi. Nonostante sia un algoritmo molto solido, il metodo RSA ha dei limiti. Ad esempio, è più lento rispetto agli algoritmi simmetrici. Nel futuro potrebbe avere grandi problemi, perché i computer quantistici possono fattorizzare numeri molto grandi in maniera molto rapida, e così RSA non sarà più sicuro come ora.

Un'altro algoritmo di crittografia a chiave pubblica basato su principi matematici simili a quelli di RSA, è ElGamal, ma esso è fondato sulla difficoltà del problema del logaritmo discreto nei campi finiti. È stato proposto negli anni Ottanta ed è ancora oggi utilizzato come base teorica per diversi protocolli crittografici, soprattutto in ambito di voto elettronico.[Min25a]

Il funzionamento di ElGamal può essere descritto attraverso i seguenti passaggi fondamentali.

1. Si sceglie un grande numero primo p e un generatore g del gruppo moltiplicativo modulo p.
2. L'utente sceglie un valore segreto x, con $1 < x < p - 1$, che rappresenta la chiave privata.
3. Viene calcolato il valore pubblico $y = g^x \mod p$.
4. La chiave pubblica è quindi $\mathrm{K}_{\mathrm{pub}} = (p, g, y)$, mentre la chiave privata è $\mathrm{K}_{\mathrm{prv}} = x$.

Anche in questo caso, ogni messaggio viene rappresentato come un numero intero $m < p$. La cifratura di un messaggio non produce un singolo valore, ma una coppia di valori cifrati.

- **Cifratura:** tramite la scelta di un valore k casuale il mittenete calcola:

$$c_1 = g^k \mod p, \quad c_2 = m \cdot y^k \mod p$$

- **Decifratura:** il destitanario tramite la chiave privata x riesce a calcolare il messaggio originale:

$$m = c_2 \cdot (c_1^x)^{-1} \mod p$$

All'interno di questo algoritmo se cifriamo lo stesso messaggio più volte con la stessa chiave pubblica, otteniamo testi cifrati differenti. Questo è possibile grazie al valore casuale k. Questa caratteristica è molto importante in contesti come il voto elettronico, dove è fondamentale evitare il collegamento tra voti uguali.

La crittografia asimmetrica ha modificato profondamente il modo in cui vengono protette le comunicazioni digitali e ha reso possibili molti dei protocolli che oggi utilizziamo e definiscono la sicurezza nella transazioni online. Sebbene il processo dell'informatica quantistica possa rappresentare una minaccia futura per entrambi gli algoritmi, il loro ruolo rimane fondamentale sia nello sviluppo della sicurezza moderna che nella comprensione delle nuove tecniche di crittografia post-quantistica, che oggi rappresentano il passo successivo nella ricerca scientifica del settore.

3.2 Crittografia Omomorfica

Una delle innovazioni piu rilevanti nell'ambito della crittografia e molto utile nel voto elettronico è la crittografia omomorfica. Consiste in una tecnica che consente di eseguire operazioni matematiche sui dati cifrati senza aver bisogno di decifrarli preventivamente. [IBM25b]

Prima della crittografia omomorfica, per poter eseguire i calcoli o analisi, i dati dovevano sempre essere prima decifrati, esponendoli a rischi. Infatti, nella maggior parte delle situazioni i dati che noi chiedevamo di elaborare dovevano necessariamente essere in chiaro e non in forma criptata, almeno per il tempo necessario per elaborarli. Questo vuol dire che i nostri dati, per alcuni momenti e per certi lassi di tempo, dovevano per forza trovarsi in chiaro, cioè potevano essere consultabili da umani o algoritmi, e di conseguenza chi deteneva ed elaborava i nostri dati, in molti casi, possedeva meccanismi e chiavi per decriptarli. Questo vincolo diventava particolarmente critico in casi come il cloud computing, dove gli utenti delegano l'elaborazione dei dati a terze parti senza però dover sacrificare la loro privacy.

La crittografia omomorfica ha risolto questo problema riuscendo ad eseguire operazioni sui dati cifrati senza mai accedere al testo in chiaro, garantendo che il risultato una volta decifrato, corrisponda al calcolo che sarebbe stato ottenuto dal dato originario. L'idea è che se un voto è cifrato con un algoritmo omomorfico è possibile sommare i voti, aggregarli e combinarli senza che nessuno possa mai conoscere il contenuto delle singole schede. Infine quando il risultato finale aggregato viene decifrato, esso corrisponde esattamente a ciò che si sarebbe ottenuto effettuando la stessa operazione sui dati in chiaro.

Possiamo effettuare un piccolo esempio pratico se l'elettore vota "1" per il candidato A e "0" per il candidato B, il sistema è in grado di sommare tutte le cifrature e ottenere il numero di voti per A, senza vedere i singoli "1" e "0".

La prima realizzazione teorica completamente omomorfica è stata proposta nel 2009 da Craig Gentry, e ha segnato un momento fondamentale nella storia della crittografia moderna. Il suo schema si basa su una costruzione complessa che utilizza strutture matematiche definite su reticoli, introducendo un meccanismo di "bootstrapping". Quest'ultimo consente di ridurre il rumore matematico che si accumula nelle operazioni crittografiche e che senza un adeguato controllo, renderebbe i risultati incomprensibili dopo un certo numero di calcoli. Sebbene la proposta originale fosse ancora inefficiente in termini di tempo e risorse ha però aperto la strada alla ricerca che negli anni ha portato a miglioramenti considerevoli e a implementazioni più praticabili. [Wik26g]

Nonostante il suo enorme potenziale e la svolta che ha portato nel modo della crittografia, la crittografia omomorfica presenta alcuni limiti. Il limite più grande è che i calcoli sui dati cifrati sono molto più lenti rispetto a quelli sui dati in chiaro e quindi richiedono una maggiore potenza di calcolo e una maggiore memoria.

Nel voto elettronico questo meccanismo è molto utile perchè inserisce la possibilità che lo scrutinio possa essere svolto da più server o commissioni esterne senza esporre le preferenze individuali, e si riduce la quantità di informazioni sensibili in circolazione, perchè i dati sono cifrati e nessuno deve mai aprire le schede singolarmente e decifrare i dati. Infine è possibile pubblicare i voti cifrati rendendo il conteggio verificabile da chiunque, senza sapere chi ha votato per cosa. Schemi come Paillier e versioni omomorfiche di ElGamal sono oggi fra i più utilizzati nei sistemi end-to-end verificabili.

3.3 Firme Digitali e Blind Signature

Molte volte si sente parlare di firma digitale, anche se non tutti sanno precisamente di cosa si tratta. Si riferisce a una firma elettronica messa in un documento elettronico per autenticarlo, esattamente come la firma su un documento cartaceo, con lo scopo di verificare la provenienza del documento e la sua integrità. Si tratta di un sistema a chiavi asimmetriche, come visto precendentemente. Il firmatario tramite la chiave privata firma il documento elettronico e chiunque abbia accesso alla chiave pubblica può leggerlo e verificarne la validità. In pratica però il documento non viene firmato nella sua interezza, ne viene calcolato un digest, ovvero il risultato di una funzione hash crittografica applicata al documento che lo trasforma in una stringa di lunghezza fissa. Tale digest è poi cifrato con la chiave privata del firmatario e il risultato rappresenta una firma digitale. Con la firma digitale quindi si garantisce che un messaggio è autentico, integro e non ripudiabile, cioè il mittente non può negare di averlo inviato. In un qualunque contesto tradizionale questo è sufficiente, ma nel voto elettronico applicare direttamente una firma digitale al voto potrebbe produrre un grave problema, ovvero rendere possibile il collegamento del voto alla persona, violando la segretezza costituzionale. [Wik26e]

Il sistema infatti deve accertarsi che l'elettore possa votare e sia effettimente lui, che voti una sola volta, ma non deve in alcun modo sapere quale sia la sua scelta e collegare la persona al voto. Per risolvere questo problema si utilizzano le blind signatures, ideate da David Chaum, una sorta di firme digitale in cui il contenuto del messaggio viene nascosto prima di essere firmato. Infatti il messaggio viene firmato in modo cieco, non conoscendone il contenuto. Spiego successivamente il funzionamento tramite un esempio: [Wik26a]

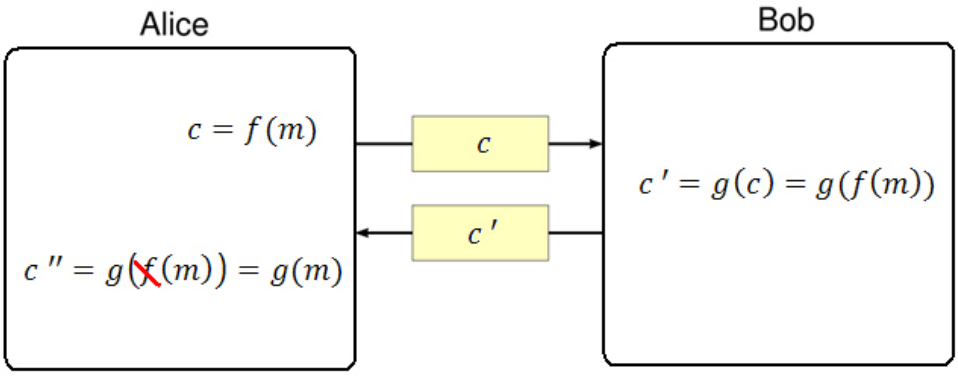

Figura 1: Esempio funzionamento blind-signature

In questo schema l'obiettivo di Alice è che Bob firmi il messaggio m senza conoscerne il contenuto. Alice quindi per nascondere il contenuto del messaggio m lo cifra con la funzione f. [Wik26a]

$$c = f(m).$$

Alice quindi invia il messaggio cifrato c a Bob. Successivamente Bob firma alla cieca il messaggio c (alla cieca perché non conosce il contenuto) attraverso una funzione g, ottenendo:

$$c' = g(c) = g(f(m)).$$

A questo punto Bob invia c' ad Alice. Alice riceve c' e rimuove la propria criptazione applicando l'inverso della funzione f, ottenendo così:

$$c'' = g(f(m)) * f^{-1} = g(m).$$

Le blind-signature quindi, nell'ambito del voto elettronico permettono a un'autorità di firmare un messaggio senza poterlo leggere. Questo metodo si basa sul concetto di "oscuramento" del dato, ottenuto applicando un fattore crittografico che nasconde il contenuto. In breve, funziona che l'elettore genera il proprio voto e lo offusca con un parametro casuale, l'autorita elettorale successivamente firma il contenuto senza poterlo visionare. Infine l'elettore rimuove l'offuscamento e ottiene una firma valida sull'originale. In questo modo l'elettore effettua un voto riconosciuto dal sistema elettorale ma non è possibile collegare la sua identità alla sua preferenza. Le blind signature quindi ci permettono di separare certificazione e anonimato, rendendo impossibile dimostrare a terzi cosa si è votato e riducendo esponenzialmente i rischi di coercizione.

3.4 Commitment Scheme

Un commitment scheme è un meccanismo per cui una persona si "impegna" su un dato senza rivelarlo, riservandosi di mostrarlo successivamente. Lo possiamo immaginare come

una busta sigillata digitale, in cui chi la riceve non vede il contenuto, ma ha la certezza che non può essere modificato. Esistono due vincoli principali che rendono possibile questo metodo. [Wik26b; Red22; Han26]

- **Binding:** chi mette il dato nella "busta" non può cambiarlo dopo.
  - Per esempio, se all'interno di una votazione, invio la mia preferenza, non posso modificarla dopo averlo trasmessa.
- **Hiding:** chi riceve la "busta" non può conoscerne il contenuto.
  - Questo vincolo all'interno delle votazioni protegge la segretezza del voto e impedisce che ci siano pressioni esterne.

Questo comportamento è incompatibile con modelli che prevedono la trasparenza immediata delle preferenze, ma perfettamente coerente con sistemi che richiedono un periodo di segretezza fino allo spoglio.

Possiamo ottenere anche la tracciabilità procedurale, perchè quando un voto viene registrato usando un commitment (la "busta chiusa digitale"):

1. Si genera una prova crittografica ovvero una specie di "impronta digitale" unica del voto, che viene salvata nel sistema.
2. Questa prova rimane memorizzata e non cambia → anche se passano giorni, mesi o anni, puoi sempre verificarla.
3. Chiunque abbia i parametri giusti può controllare in un secondo momento se il voto originale corrisponde alla prova registrata:
   - Se la prova coincide → il voto è integro.
   - Se la prova non coincide → il voto è stato alterato o modificato.

Il commitment rappresenta quindi una forma di garanzia tecnica che non dipende da enti fidati ma da meccanismi matematici oggettivi e riproducibili.

Dal punto di vista tecnico, i sistemi di commitment si fondano su primitive crittografiche come funzioni hash o algoritmi a chiave pubblica. Nel caso di un hash, l'elettore invia il digest della propria preferenza insieme a un valore casuale, noto come "nonce" o parametro di mascheramento. Questo valore aggiuntivo garantisce che due voti identici non generino lo stesso commitment, evitando confronti diretti da parte dell'autorità o di eventuali osservatori. Quando arriva il momento della verifica, l'elettore rivela sia la preferenza sia il parametro utilizzato. Se l'hash calcolato coincide con quello registrato nella fase iniziale, il voto è considerato autentico e non alterato. [Pia26a]

$$\underbrace{\text{Voto } (m)}_{\substack{\text{scelta}\\ \text{dell'elettore}}} + \underbrace{\text{Nonce } (r)}_{\substack{\text{numero casuale}\\ \text{per mascherare}\\ \text{il voto}}} \longrightarrow \underbrace{\text{Digest } H(m,r)}_{\substack{\text{impronta digitale}\\ \text{unica del voto,}\\ \text{H funzione hash}}} \longrightarrow \underbrace{\text{Registrazione nel sistema}}_{\substack{\text{memorizzazione sicura}\\ \text{del commitment}}}$$

Per effettuare la verifica l'elettore rivela m e r, il sistema calcola $H(m, r)$ e lo confronta con il digest registrato. Se coincidono, il voto è autentico e integro.

Esiste anche altro approccio che si basa su algoritmi crittografici a chiave asimmetrica: il votante cifra il valore del voto con una funzione facilmente verificabile ma non invertibile senza conoscere il contenuto.

$$\underbrace{\text{Voto } (m)}_{\text{scelta dell'elettore}} \longrightarrow \underbrace{\text{Cifratura } E(m, \text{parametri})}_{\substack{\text{funzione verificabile senza}\\ \text{rivelare il contenuto,}\\ \text{E} \rightarrow \text{funzione di cifratura a}\\ \text{chiave pubblica}}} \longrightarrow \underbrace{\text{Registrazione nel sistema}}_{\substack{\text{memorizzazione sicura del}\\ \text{commitment}}}$$

L'impiego dei Commitment Scheme nel voto elettronico dimostra come sia possibile coniugare sicurezza e riservatezza senza sacrificare la verificabilità dei risultati. La protezione del voto è affidata a strumenti crittografici solidi, mentre la trasparenza complessiva del processo rimane integra, permettendo controlli sia automatici sia manuali. In questo senso il commitment non è solo un elemento tecnico, ma un tassello fondamentale per costruire sistemi elettorali digitali che mantengano le stesse garanzie del voto tradizionale e, in molti casi, ne rafforzino l'affidabilità strutturale.

3.5 Zero-Knoweledge Proofs (ZKP) o Prove a conoscenza zero

Le Zero-Knowledge Proofs sono uno strumento crittografico molto importante per garantire sicurezza e trasparenza nei sistemi di voto elettronico. Il principio di base è: un soggetto deve poter dimostrare la validità di un'informazione senza rivelare quale sia l'informazione. [KNO23]

Il funzionamento si basa su protocolli che permettono a un soggetto, detto *prover*, di dimostrare la veridicità di un'informazione a un altro soggetto, detto *verifier*, senza rivelare l'informazione stessa.

- **Prover:** è in possesso di un'informazione segreta (come può essere il contenuto di un voto).
- **Verifier:** ha il compito di verificare che l'informazione sia corretta senza conoscerla.

Nell'ambito del voto elettronico, le zero-knowledge proofs o prove a conoscenza zero, sono molto importanti perchè permettono di dimostrare che:

- il voto è corretto, ovvero appartiene all'insieme delle scelte possibili;
- il voto è stato cifrato in maniera corretta;
- il voto è univoco, ovvero è stato registrato una sola volta.

Grazie all'utilizzo delle zero-knowledge proofs si riesce a dimostrare tutte queste caratteristiche senza dover rivelare la prefernza espressa dall'elettore.

$$\text{Elettore (Prover)} \quad \longrightarrow \quad \text{Prova ZK} \quad \longrightarrow \quad \text{Sistema di verifica (Verifier)}$$

Il sistema di controllo verifica la correttezza della prova senza accedere al contenuto del voto, per mantenere la segretezza del voto.

Un ulteriore vantaggio delle zero-knowledge proofs è la protezione contro coercizione e compravendita del voto. Dato che l'elettore non è in grado di dimostrare quale voto abbia espresso, diventa impossibile esercitare pressioni o richiedere prove del voto espresso..

Le zero-knowledge proofs rappresentano quindi uno strumento fondamentale nei sistemi di voto elettronico moderni, poiché consentono di verificare la correttezza del processo elettorale senza compromettere l'anonimato degli elettori.

Nonostante questi vantaggi, anche le zero-knowledge proofs presentano dei limiti. Da un lato bisogna prevedere protocolli che siano efficienti dal punto di vista computazionale, poiché la generazione e la verifica delle prove deve essere compatibile con un numero elevato di votanti e con tempistiche tipiche di una consultazione elettorale reale. Dall'altro lato, occorre che il sistema normativo riconosca la validità delle prove matematiche nella certificazione del voto, mettendo insieme i modelli crittografici con procedure amministrative e giuridiche. Quindi nel passaggio dal voto tradizionale a quello digitale c'è bisogno anche di una maturazione delle istituzioni.

In definitiva, grazie alle zero-knowledge proofs, un elettore può partecipare alla consultazione senza cedere il controllo sui propri dati e allo stesso tempo la collettività ottiene una forma di controllo verificabile che rafforza la fiducia nel risultato elettorale. Si tratta di una soluzione che, pur essendo tecnicamente complessa, offre una sintesi efficace tra le esigenze della segretezza democratica e la necessità di rendere verificabili i meccanismi di decisione collettiva.

3.6 Ruolo complessivo della crittografia nel voto elettronico

Per quanto riguarda il contesto del voto digitale, la crittografia non è solo una componente accessoria ma la struttura portante dell'intero modello elettorale. Se nel voto tradizionale

la garanzia dell'integrità del processo può essere affidata a scrutatori, osservatori di lista, presidenti di seggio, etc, nel voto elettronico questa fiducia viene sostituita o integrata da meccanismi matematici verificabili da chiunque.

Grazie alle tecniche che sono illustrate precedentemente è possibile rendere il voto anonimo e non riconoscibile, assicurare che solo gli aventi diritto possano votare, impedire il voto multiplo, pubblicare dati verificabili senza rivelare i voti individuali, infine consente a chiunque di controllare la correttezza matematica dell'esito. In altre parole, mentre nel sistema tradizionale la fiducia è umana e procedurale nel voto elettronico tende a diventare scientifica e dimostrabile, fondata su prove formali, non contestabili e universalmente verificabili.

4 Paradigmi dei sistemi di voto elettronico

La realizzazione e l'evoluzione del voto elettronico portò alla definizione di diversi modelli progettuali, ciasciuno di essi è nato per rispondere con approcci differenti ai requisiti fondamentali di un voto elettronico democratico, come abbiamo già visto precedentemente: anonimato, integrità, verificabilità e protezione contro una possibile coercizione. Ad oggi non esiste un modello o un'architettura che viene riconosciuta come migliore, ciascuna con punti di forza e limiti differenti.

Tra i paradigmi più rilevanti vedremo successivamente sistemi basati su mix-nets, sistemi basati sulla crittografia omomorfica, sistemi End-to-End verifiable (E2E) e infine sistemi ibridi e blockchain-based. Nei prossimi paragrafi cercherò di analizzarli nel dettaglio, spiegando pregi e difetti di ognuno, con particolare attenzione al modo in cui realizzano i principali requisiti del voto digitale.

4.1 Sistemi basati su mix-nets

Le mix networks, o mix-nets, rappresentano uno dei primi approcci matematici ideati per garantire l'anonimato in un sistema di voto elettronico. Ideate alla fine degli anni 80, si basano su un'idea semplice: se si prende una sequenza di voti cifrati e la si invia attraverso una catena di server indipendenti, ognuno dei quali li rimescola e li ricifra, è possibile produrre una sequenza finale che non può essere collegata agli elettori originali. Il processo funziona che gli elettori inviano i propri voti cifrati a un primo server chiamato "mix node", il server li rimescola, li ricifra e li passa al nodo successivo, al termine della catena, la lista viene pubblicata e i voti possono essere decifrati e conteggiati. Infine per garantire trasparenza, ogni nodo fornisce una prova crittografica che dimostra di aver eseguito correttamente le operazioni di rimescolamento, senza alterare il contenuto dei voti. [Wik26i; Lak20]

I sistemi mix-nets possono essere implementati mediante diverse tecniche crittografiche, ma il modello più diffuso utilizza la cifratura a chiave pubblica con ricifratura successiva. Ogni nodo prende ogni voto cifrato, applica una trasformazione crittografica tale da mantenerne il contenuto invariato, e infine rilascia la nuova versione del messaggio insieme allo scambio dell'ordine dei voti.

Si consideri una votazione con tre elettori E_1, E_2, E_3, che esprimono rispettivamente i voti V_1, V_2, V_3. Ogni elettore cifra il proprio voto utilizzando la chiave pubblica del sistema e lo invia all'infrastruttura di voto. La sequenza iniziale dei voti cifrati risulta quindi ordinata come:

$$(C(V_1), C(V_2), C(V_3))$$

Il primo nodo della mix-net riceve l'insieme dei voti cifrati, ne modifica l'ordine mediante una permutazione casuale e applica una ricifratura, producendo ad esempio la sequenza:

$$(C'(V_2), C'(V_3), C'(V_1))$$

accompagnata da una prova crittografica che dimostra la correttezza dell'operazione senza rivelare la permutazione adottata. Il secondo nodo ripete lo stesso procedimento, generando un'ulteriore permutazione e ricifratura dei voti.

Al termine della catena di nodi, la sequenza finale dei voti cifrati non è più correlabile all'ordine originale di invio. Solo a questo punto i voti vengono decifrati e sottoposti a scrutinio, garantendo sia la correttezza del risultato finale sia la completa separazione tra identità dell'elettore e voto espresso.[Ver26]

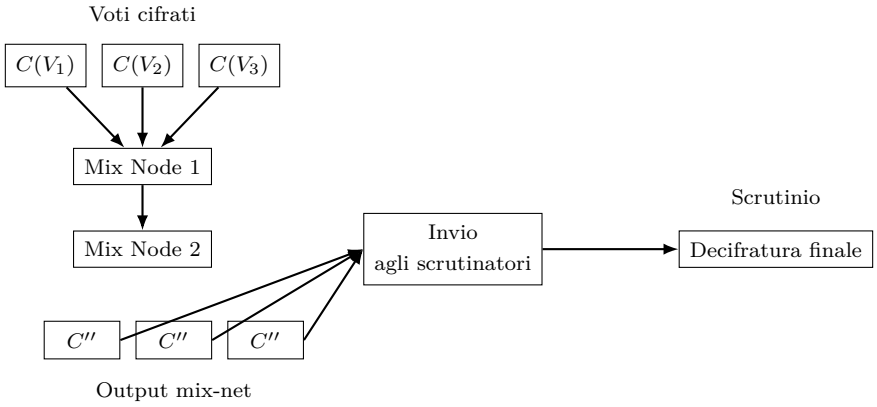

Figura 2: Schema completo di una mix-net: permutazione e ricifratura dei voti seguite dalla decifratura finale.

Come possiamo immaginare nel contesto del voto elettronico, le mix-nets vengono utilizzate principalmente nella fase di scrutinio. Gli elettori compilano una scheda utilizzzando la chiave pubblica del sistema e depositano il proprio voto. La registrazione di queste schede può essere resa pubblica, purchè rimanga cifrata, così da permettere a tutti

di verificare che nessun voto sia stato rimosso o aggiunto successivamente. Solo dopo la raccolta totale inizia il processo di miscelazione attraverso la rete di nodi, fino alla produzione finale delle schede decifrate, che ora risultano anonime e non più riconducibili agli elettori di partenza. Da questo momento il conteggio avviene in chiaro, in modo da consentire il controllo pubblico dei risultati finali e la certezza che tutte le schede registrate prima siano effettivamente presenti dopo la procedura di anonimizzazione.

Infine possiamo dire che questo paradigma ha numerosi pregi, ovvero riesce a separare completamente l'identità dell'elettore dal suo voto, consente agli osservatori esterni di verificare matematicamente la correttezza del processo, e non richiede la fiducia dell'autorità, perchè ogni nodo è controllabile. Nonostante la solidità matematica, le mix-nets presentano alcuni limiti: richiedono una capacità computazionale molto elevata soprattutto in caso di elezioni su larga scala, se anche un solo nodo è compromesso e non fornisce le prove corrette, l'intero processo deve essere invalidato, e non ci sono controlli in caso di malware sul dispositivo dell'elettore. Nonostante questi limiti resta uno dei modelli più adottati nei sistemi accademici e istituzionali.

4.2 Sistemi homomorphic

Una seconda famiglia importante è rappresentata dai sistemi che utilizzano e sfruttano la crittografia omomorfica, cioè, come abbiamo visto, algoritmi che permettono di effettuare operazioni sui voti cifrati senza doverli mai decifrare singolarmente. [Wik26h] In un'elezione, ad esempio, i voti possono essere cifrati in modo che la somma dei valori cifrati corrisponda, una volta decifrata al totale reale dei voti registrati. Questo può significare che il sistema può rendere pubblici tutti i voti cifrati, permettendo a chiunque di partecipare alla somma, e solo alla fine decifrare il totale. Rimanendo segreta la preferenza individuale di ogni elettore.

Un ulteriore aspetto rilevante riguarda la gestione della chiave privata finale, necessaria per la decifratura del risultato complessivo. Per impedire che un singolo soggetto possa controllare o manipolare lo scrutinio, la chiave non viene affidata a una sola entità ma divisa in più frammenti, ciascuno assegnato a un organismo diverso, spesso appartenente a istituzioni scollegate tra loro. Solo la combinazione di tutte le parti permette di rivelare l'esito dell'elezione. Questo modello garantisce che nemmeno il soggetto incaricato della decodifica possa riconoscere i singoli voti, mantenendo la separazione ideale tra gestione operativa e conoscenze delle preferenze individuali. [KHC22b]

Per chiarire il funzionamento, nella Figura sottostante mostro uno schema semplificato dello scrutinio omomorfico.

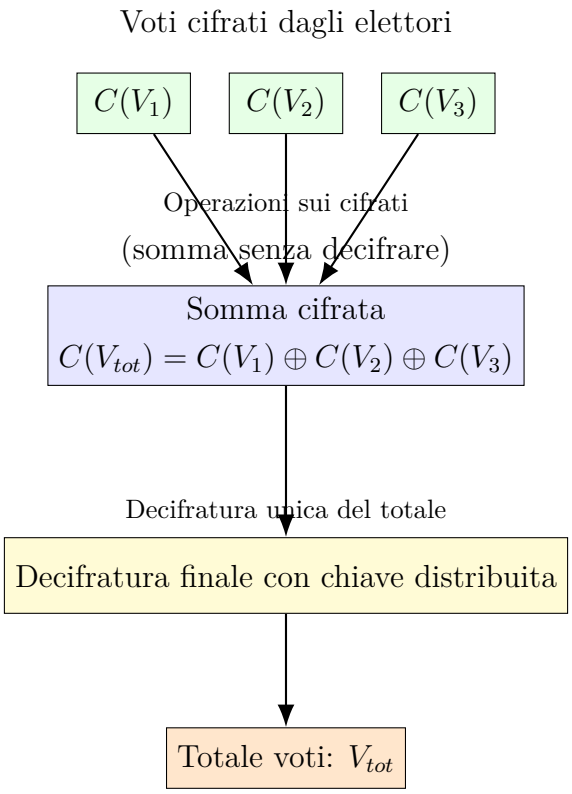

Figura 3: Esempio semplificato di scrutinio omomorfico: i voti cifrati possono essere combinati senza decifrarli singolarmente e la decifratura finale produce solo il totale.

I sistemi omomorfici presentano caratteristiche particolarmente interessanti: nessuno deve mai decifrare i voti singolarmente, riducendo il numero di punti vulnerabili, è possibile ottenere uno scrutinio pubblico e verificabile da terze parti, ed eventuali autorità, server o osservatori possono partecipare al conteggio senza venire in contatto con dati sensibili. Sono quindi molto efficaci per il requisito di universal verifiability, poichè l'intero processo matematico è trasparente. Tuttavia come tutti i modelli presenta alcune criticità: si basa su algoritmi complessi che richiedono competenze avanzate da parte dei controllori, il sistema deve assicurare che ogni voto cifrato rappresenti una scelta valida e non sempre gestiscono agevolmente schede con molte opzioni, preferenze o voto disgiunto. Molti sistemi moderni, tra cui diversi prototipi europei e statunitensi, adottano schemi omomorfici proprio per la loro trasparenza matematica. [Fon26]

4.3 Sistemi End-to-End Verifiable (E2E)

I sistemi End-to-End Verifiable rappresentano oggi un pilastro nell'ambito del voto elettronico. L'obiettivo è quello di creare un'elezione che non richieda la fiducia nell'autorità elettorale, perchè ogni fase è possibile verificarla da chiunque, esperti e non. [Wik26d]

Un sistema è considerato E2E se garantisce contemporaneamente la verifica individuale, la verifica universale e la segretezza della preferenza. In altre parole, nella verifica

individuale, l'elettore può controllare che il proprio voto sia stato registrato correttamente e sia stato incluso nel conteggio finale. Nella verifica universale, chiunque, anche un osservatore esterno senza privilegi, può verificare la correttezza dello scrutinio. La segretezza della preferenza, come si può intuire, consiste nel fatto che nessuno possa essere in grado di risalire al contenuto del voto del singolo elettore. [IBM26]

Per raggiungere tutto questo, i sistemi E2E combinano tipicamente: crittografia asimmetrica, crittografia omomorfica o mix-nets, commitment e prove a conoscenza zero. L'elettore riceve spesso uno "scontrino crittografico" contenente informazioni che permettono la verifica futura. Questo scontrino non rivela il voto, ma consente di controllare che il server non lo abbia alterato e abbia contato il suo voto nello scrutinio finale. Questo meccanismo risolve un problema storicamente rilevante del voto elettronico: la percezione di opacità del processo. Mentre nel voto su carta l'elettore può osservare materialmente la propria scheda depositata nell'urna, nel voto digitale l'unica garanzia consiste nella trasparenza crittografica. Il cittadino può verificare la presenza della propria ricevuta all'interno dell'elenco pubblico dei voti registrati, assicurandosi che non sia stata cancellata, alterata o duplicata. Allo stesso tempo, il fatto che la ricevuta non permetta a un terzo di capire per chi è stato espresso il voto impedisce qualsiasi forma di coercizione o di compravendita della preferenza.

Nella Figura sottostante mostro uno schema semplificato di un sistema End-to-End Verificable, considerando una votazione con tre elettori E_1, E_2, E_3, che esprimono rispettivamente i voti v_1, v_2, v_3 (per semplicità sì/no, 1 o 0).

1. Commitment: tramite l'utilizzo di un commitment crittografico $C(v_i, r_i)$ ogni elettore "sigilla" il proprio voto. r_i è un numero casuale scelto dall'elettore. Come abbiamo visto precedentemente il commitment funziona come una "busta sigillata". Ad esempio:
$$C(v_i, r_i) = H(v_i \,||\, r_i)$$
dove H è una funzione hash sicura.

2. Zero-Knowledge Proof (ZKP): ogni elettore grazie all'utilizzo delle ZKP genera una prova crittografica che il voto è valido senza doverlo rivelare. ZKP$(C(v_i, r_i))$

3. Crittografia dei voti e combinazione: i commitment vengono trasformati in voti cifrati operabili matematicamente, ad esempio con crittografia omomorfica:
$$E(v_i) = g^{v_i} h^{r_i} \mod p$$
I voti cifrati possono essere combinati direttamente per ottenere il totale cifrato:
$$E(V_{\text{tot}}) = \prod_{i=1}^{3} E(v_i) = g^{v_1+v_2+v_3} h^{r_1+r_2+r_3} \mod p$$

senza mai rivelare i voti singoli.

4. Decifratura finale: solo nel momento dello scrutinio, tramite l'utilizzo della chiave privata si può decifrare il totale. Spesso la chiave privata per sicurezza viene distribuita tra più autorità.

$$V_{\text{tot}} = \text{Dec}(E(V_{\text{tot}})) = v_1 + v_2 + v_3$$

Tramite questo sistema si riesce a garantire **riservatezza dei voti individuali**, **verificabilità matematica** e **trasparenza crittografica** dell'esito.

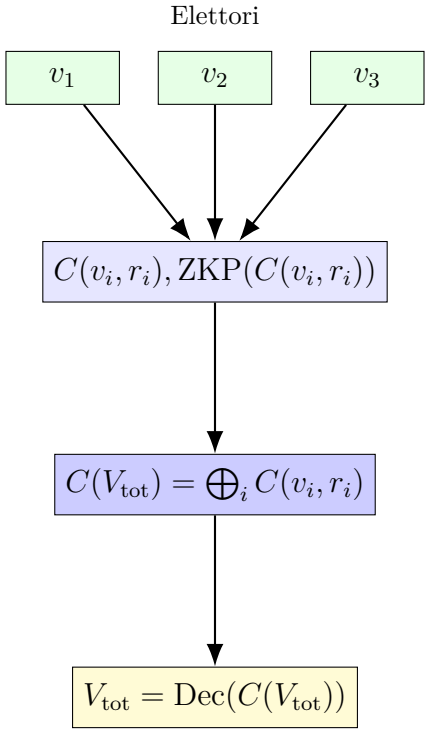

Figura 4: Schema di un sistema E2E.

Il più grande vantaggio dei sistemi E2E è che evitano che l'elezioni si trasformino in un atto "di fiducia cieca" verso chi la gestisce, potendo dimostrare in autonomia la correttezza matematica. Questi sistemi presentano però alcune complicazioni: sono più difficili da spiegare all'elettore medio, richiedono implementazioni rigorose e trasparenti. Nonostante il sistema sia stato progettato per essere semplice e comprensibile dall'elettore attraverso pochi passaggi, comprendere ciò che avviene dietro le quinte può risultare complesso. Un limite come abbiamo già visto è la ricevuta crittografica, che non deve essere possibile dimostrare a terzi la scelta del voto, altrimenti introdurrebbe problemi come la coercizione. Molte delle soluzioni più avanzate oggi sperimentali o implementate, tra cui Helios, Pret a Voter e ElectionGuard, che vedremo successivamente, si basano proprio su questo paradigma.

4.4 Sistemi ibridi e blockchain-based

Negli ultimi anni sono stati proposti sistemi di voto elettronico che combinano più paradigmi crittografici già esistenti, integrandoli con infrastrutture distribuite ispirate alla tecnologia blockchain. Questi sistemi, definiti ibridi, non introducono nuovi meccanismi crittografici fondamentali, ma utilizzano strumenti consolidati come crittografia asimmetrica, schemi omomorfici, mix-nets, commitment e prove a conoscenza zero, collocandoli all'interno di un registro distribuito e immutabile.

L'idea centrale non è quella di memorizzare il voto in chiaro sulla blockchain, bensì di utilizzare la blockchain come bacheca pubblica, ossia come un registro in cui è possibile solo aggiungere informazioni che garantiscono integrità, trasparenza e disponibilità delle informazioni crittografiche. In questo modello, sulla blockchain vengono pubblicati esclusivamente artefatti crittografici, come voti cifrati, commitment, ricevute e prove di correttezza, mentre la segretezza della preferenza è garantita dagli schemi crittografici sottostanti.[Yi19]

Dal punto di vista funzionale, i sistemi basati su blockchain si inseriscono naturalmente nel paradigma End-to-End Verifiable. Ogni elettore può verificare che il proprio voto cifrato sia stato correttamente registrato nel registro distribuito, mentre gli osservatori esterni possono controllare la correttezza dello scrutinio finale verificando le prove crittografiche pubblicate. L'immutabilità del registro impedisce la cancellazione o la modifica retroattiva dei voti, rafforzando il requisito di integrità. [Lar+21]

Un aspetto importante riguarda la distinzione tra consenso blockchain e sicurezza del voto. Il meccanismo di consenso garantisce che il registro sia coerente e condiviso, ma non fornisce di per sé segretezza o correttezza del voto. Tali proprietà dipendono esclusivamente dai protocolli crittografici di voto, mentre la blockchain funge da infrastruttura di pubblicazione e in cui è possibile revisionare i voti.

Prendiamo come nel capitolo precendente l'esempio di una votazione con tre elettori E_1, E_2, E_3, che rispettivamente esprimono i voti v_1, v_2, v_3. Ogni elettore:

- cifra il proprio voto utilizzando la chiave pubblica,
- successivamente genera un commitment e una prova a conoscenza zero per dimostrare la validità del voto,
- infine pubblica il voto cifrato e le prove sulla blockchain.

Il registro distribuito da la possibilità di rendere pubblici e non mutabili tutti i voti cifrati. Lo scrutinio avviene solo dopo la pubblicazione, e tramite crittografia omomorfica o mix-nets.

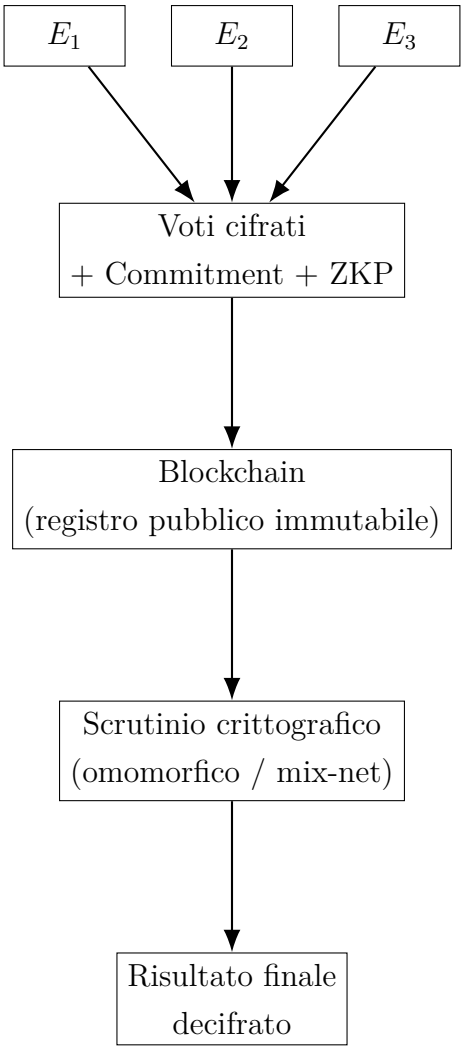

Figura 5: Schema concettuale di un sistema di voto blockchain-based.

I principali vantaggi di questi sistemi risiedono nella trasparenza, nell'immutabilità dei dati e nella facilità di revisione pubblica. Tuttavia, essi presentano anche limiti significativi: la complessità implementativa, i costi computazionali, i problemi di scalabilità e il rischio di confondere la sicurezza del consenso blockchain con la sicurezza del voto vero e proprio. Per questo motivo, la blockchain non deve essere considerata una soluzione autonoma, ma piuttosto un componente infrastrutturale che può rafforzare sistemi di voto crittografico già solidi.[Par+21]

4.5 Conclusioni

In questo capitolo ho cercato di presentare e analizzare i principali paradigmi di voto elettronico. Ne emerge che non esiste un sistema di voto elettronico perfetto e ottimale, ma una serie di soluzioni che hanno proprietà e limiti differenti a seconda del contesto e delle minacce considerate, si può scegliere il più adatto.

I sistemi basati sulle mix-nets vengono utilizzati principalmente quando si punta a garantire l'anonimato del voto attraverso una serie di rimescolamenti crittografici e decifrature distribuite. Questo approccio riesce ad avere una forte separazione tra elettore e voto espresso, ma riscontra una forte complessità computazionale, che porta a una minore fiducia nelle autorità coinvolte.

I sistemi omomorfici risultano molto interessanti perchè danno la possibilità di sommare i voti cifrati senza doverli decifrare. Facendo ciò possiamo cifrare singolarmente ogni singolo voto, sommare tutti i voti cifrati, e in fase di scrutinio decifrare direttamente la somma totale dei voti, senza esporre la preferenza del voto. Questo tipo di sistemi hanno bisogno però di meccanismi aggiuntivi per garantire la correttezza dei voti espressi.

I sistemi End-to-End Verifiable (E2E) rappresentano un'evoluzione significativa rispetto agli approcci tradizionali, in quanto permettono agli elettori e agli osservatori esterni di verificare l'intero processo di voto, dalla corretta registrazione del voto fino allo scrutinio finale. Questo paradigma utilizza primitive crittografiche avanzate, come commitment scheme e prove a conoscenza zero, migliorando la trasparenza complessiva del sistema senza compromettere la segretezza del voto. Ha invece come limite, l'elevata complessità concettuale e implementativa che può incidere negativamente sull'usabilità del sistema.

Infine abbiamo visto e analizzato brevemente i sistemi ibridi e blockchain-based. Questi sistemi si caratterizzano per la particolarità di combinare più elementi diversi tra loro. I sistemi basati sulle blockchain combinano elementi dei paradigmi visti in precedenza con l'uso di registri distribuiti, in cui la blockchain svolge il ruolo di bacheca pubblica immutabile.

Infine tramite quest'analisi possiamo concludere che la sicurezza di un sistema di voto elettronico non può essere affidata unicamente a una singola tecnologia, ma richiede una progettazione più amplia che integri più strumenti crittografici. L'utilizzo di un determinato paradigma rispetto a un'altro dipende dal contesto elettorale, dalla fiducia nell'autorità coinvolta e soprattutto dai requisiti che sono richiesti dal sistema di voto che vogliamo realizzare.

5 Analisi dei sistemi crittografici nei diversi paesi

Il tipo di sistema di voto elettronico adottato in ogni paese varia a seconda delle normative, della cultura e delle tecnologie presenti. In particolare, la crittografia non viene utilizzata sempre allo stesso modo: alcuni Stati la utilizzano come semplice strumento di protezione dei dati, mentre altri la pongono al centro del modello del processo elettorale. Nei sistemi più avanzati, la crittografia non è limitata alla sola fase di trasmissione del voto, ma viene impiegata per garantire la segretezza della preferenza, l'integrità del voto, la verificabilità individuale e universale e, in alcuni casi, la resistenza alla coercizione. In altri contesti, invece, il voto elettronico ha un utilizzo più limitato di tecniche crittografiche avanzate.

5.1 Estonia (i-voting nazionale)

L'Estonia è stato uno dei primi paesi ad adottare un sistema di voto elettronico via Internet per le elezioni politiche. Il sistema è noto con il nome i-voting ed è in uso dal 2005, consente agli elettori di votare da qualsiasi computer connesso alla rete. [Sta26]

Procedura di voto e sicurezza crittografica:

La procedura di voto elettronico inizia con l'elettore che si autentica con strumenti che identificano la propria identità allo stato, quali la carta d'identità elettronica (e-ID), Mobile-ID o Smart-ID, fornendo certificati digitali e PIN per l'autenticazione e firma digitale e successivamente l'elettore può votare. Dopo aver selezionato la propria preferenza, un algoritmo crittografico asimmetrico la cifra con la chiave pubblica delle elezioni stabilita dalla National Electoral Committee. Il voto cifrato viene quindi firmato dall'elettore tramite la firma digitale e trasmesso al server di raccolta dati. [Sta26]

Al contempo, un servizio di registrazione indipendente appone un timestamp e registra i voti ricevuti, consentendo la verifica successiva che ogni voto sia stato inoltrato correttamente. La firma digitale associata al voto viene poi rimossa prima della fase di conteggio, separando così l'identità dell'elettore dalla preferenza espressa. [Sta26] Nel conteggio dei voti, gli schemi crittografici implementano talvolta processi di mixing o di de-associazione per aumentare l'anonimato, seguiti dalla decifratura delle schede cifrate utilizzando la chiave privata elettorale, che è detenuta in modo distribuito tra i membri del comitato elettorale per ridurre i rischi associati a compromissioni singole. [ERR23]

Prima e dopo le elezioni, l'intero sistema è soggetto a verifiche e controlli indipendenti, compresi esami da parte di organismi internazionali come l'OSCE/ODIHR e controlli di sicurezza commissionati dal governo estone, ad esempio dalle società di revisione certificate. Gli elettori possono inoltre verificare che il proprio voto sia stato ricevuto correttamente mediante appositi strumenti di verifica offerti dallo Stato.[ERR23]

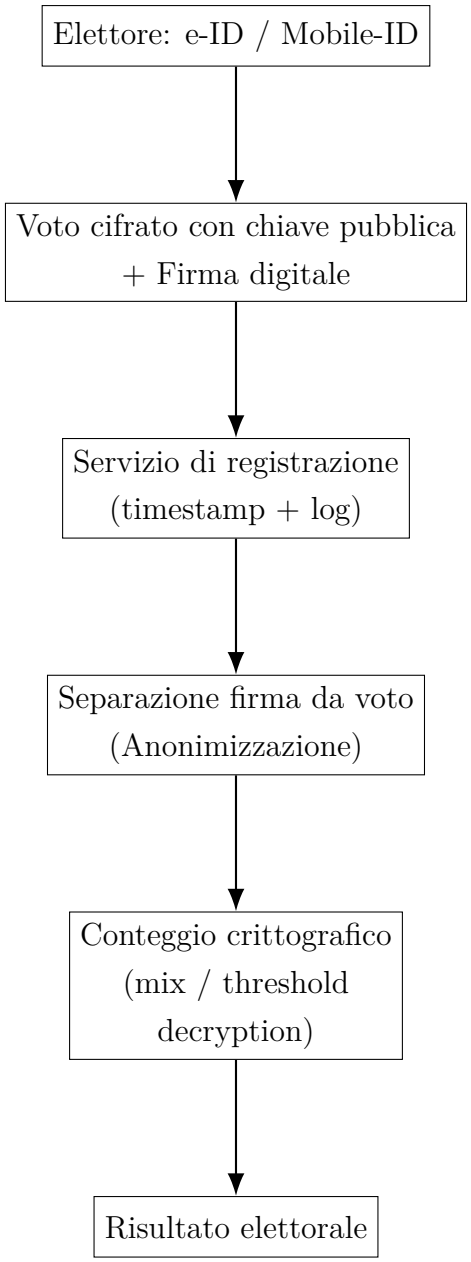

Figura 6: Schema semplificato del processo i-voting in Estonia: autenticazione, cifratura, registrazione, anonimizzazione e conteggio crittografico.

Criticità e affidabilità:

Nonostante questo sistema venga utilizzato da tanti anni, non è privo di critiche. Vari studi e rapporti accademici evidenziano delle possibili vulnerabilità, legate principalmente alla fiducia nei server centrali che hanno il compito di conteggiare i voti e alla sicurezza del software, facendo notare che una possibile compromissione di questi componenti potrebbe alterare i risultati e rendere il voto invalidante. Tuttavia, la combinazione tra identità digitale statale, crittografia asimmetrica, firme digitali e controlli regolari contribuisce a rendere il sistema uno dei pochi casi di e-voting nazionale realmente utilizzati in ambito

politico su larga scala.[Ind14]

5.2 Svizzera (swiss post)

La Svizzera è uno dei paesi europei che ha condotto sperimentazioni di voto elettronico, con un approccio che unisce crittografia avanzata e controlli indipendenti. I sistemi di e-voting svizzeri non si limitano a garantire la trasmissione sicura delle preferenze, ma cercano di fornire anche verificabilità e trasparenza, pur mantenendo la segretezza del voto come requisito fondamentale.

Architettura e contesto:

L'obiettivo iniziale per cui è stato avviato il sistema di e-voting svizzero è estendere la partecipazione elettorale per i cittadini residenti all'estero, riducendo così i tempi e i costi di logistica associati al voto per corrispondenza. E' stato così sviluppato il sistema in collaborazione con operatori tecnici specializzati, tra cui la Swiss Post, che è il sistema di posta svizzero. Questo sistema adotta un approccio ibrido: prima della votazione, l'elettore riceve per posta una busta contenente i codici di voto e le credenziali necessarie per accedere al sistema di e-voting. [Swi26]

Il sistema di voto elettronico svizzero utilizza principalmente 3 degli strumenti crittografici visti precedentemente:

- Cifratura asimmetrica dei voti: il voto espresso dell'elettore viene cifrato con chiave pubblica elettorale prima di trasmetterlo ai server centrali.
- Commitment e prove a conoscenza zero (ZPK): l'utilizzo di questi paradigmi, come abbiamo visto, garantisce la correttezza della cifratura e dei voti, senza doverne rivelare il contenuto.
- Rimescolamento e anonimizzazione: si rimescolano i voti e si anonimizzano, per evitare la correlazione tra il voto cifrato e l'elettore. Solo successivamente si effettua il conteggio.

[Pia26c]

Un elemento che caratterizza l'e-voting svizzero, è il forte controllo del processo. Prima di ogni elezione o referendum in cui viene utilizzato questo sistema, vengono eseguiti:

- Test di sicurezza ufficiali, condotti da enti esterni qualificati.
- Revisione delle componenti software e dei protocolli crittografici.
- Pubblicazione dei rapporti di controllo che documentano l'affidabilità delle procedure.

[Pia26b]

Criticità e affidabilità :

Nonostante i numerosi sforzi, sia in ambito tecnico che organizzativo, l'e-voting in Svizzera è stato molto spesso oggetto di dibattiti politici che richiedevano ulteriori garanzie di trasparenza. Alcuni Cantoni hanno deciso di sospendere l'utilizzo dell'e-voting di fronte a segnalazioni sul potenziale rischio di manipolazioni e vulnerabilità.

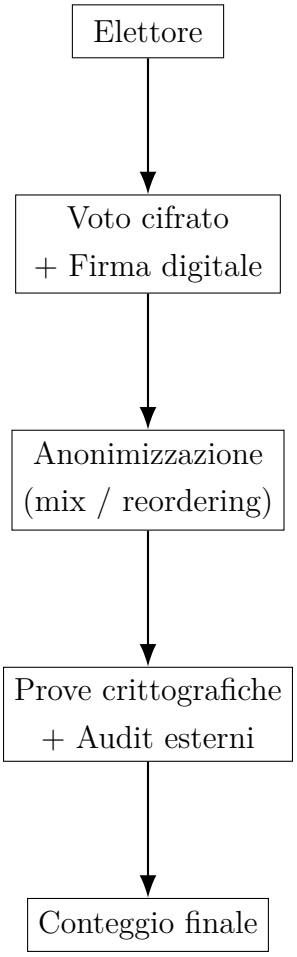

Figura 7: Schema del processo di e-voting in Svizzera.

5.3 Brasile (urne elettroniche)

Il voto elettronico in Brasile è ormai utilizzato sin dal 1996, anno in cui furono introdotte le cosiddette *urnas eletrônicas*, per modernizzare e rendere più sicure le elezioni. [Wik26c]

Architettura tecnica delle urne elettroniche:

Le urne elettroniche utilizzate in Brasile sono dei dispositivi, di tipo DRE (Direct Recording Electronic), ovvero microcomputer che si occupano di raccogliere e archiviare i

voti in locale. Il processo di voto si svolge sul terminale fisico presso il seggio elettorale in cui l'elettore esprime il proprio voto tramite un'interfaccia touch o tastiera, e la macchina registra la scelta nella memoria locale. Al termine di ogni giornata elettorale, la macchina genera una tabulazione dei risultati raccolti e invia in modo sicuro una copia alle sedi centrali, che si occuperanno della somma complessiva dei voti. Una particolarità di questo sistema è che durante il voto presso il seggio elettorale non è presente connessione a Internet, le operazioni di voto e la registrazione avvengono in locale sulla macchina. [Wik26c]

Per garantire la correttezza del processo, il Tribunal Superior Eleitoral, ovvero la corte elettorale superiore organizza regolarmente test pubblici di sicurezza in cui esperti esterni sono invitati ad esaminare ed attaccare le urne alla ricerca di vulnerabilità. Questi test ripetuti periodicamente, permettono di identificare punti deboli del sistema e di adottare contromisure. [Wik26k]

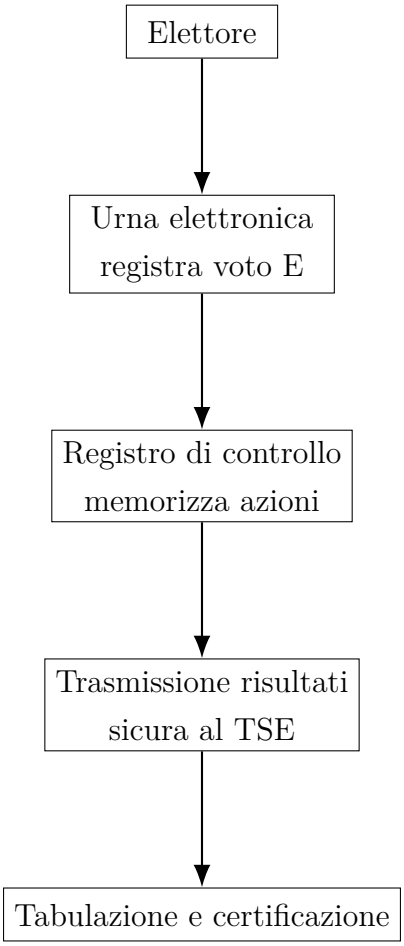

Figura 8: Schema semplificato del processo delle urne elettroniche brasiliane.

Molti sistemi tra cui quelli visti precedentemente pubblicano prove crittografiche verificabili da terzi, le urne brasiliane si affidano invece a:

- procedure di test e controlli esterni,

- controllo fisico delle apparecchiature,
- trasmissione sicura dei risultati aggregati.

Questa modalità non fornisce al singolo elettore strumenti crittografici per verificare matematicamente che il proprio voto sia stato incluso correttamente nello scrutinio finale.

Nonostante questo sistema sia in uso da tanto tempo, esistono tutt'ora lunghi dibattiti in cui le figure politiche mettono in discussione l'affidabilità delle urne elettroniche e le istituzioni difendono la robustezza complessiva dell'apparato elettorale brasiliano. Nonostante ciò, le autorità giudiziarie e i controlli elettorali hanno respinto varie richieste di annullamento dei risultati basate su presunti brogli, sottolineando l'assenza di prove concrete di manipolazione sistemica. [Eur22; Il 25]

5.4 Stati Uniti (Election Guard)

Negli Stati Uniti è stato trattato spesso il concetto di voto elettronico sia a livello federale che localmente tramite iniziative. Tra le varie iniziative uno degli sviluppi più significativi a livello crittografico è rappresentato da ElectionGuard, un framework open source messo a disposizione da Microsoft per implementare proprietà di End-to-End Verifiability in sistemi di voto elettronico. [Ele26]

ElectionGuard non riguarda un sistema elettorale, ma una libreria software che può essere integrata nei sistemi di voto. L'obiettivo è quello di consentire agli elettori o alle autorità di controllo di confermare che:

- ogni voto espresso sia stato ricevuto correttamente,
- ogni voto sia stato incluso nel conteggio finale,
- nessun voto legittimo sia stato escluso o alterato.

[Fre26]

Queste proprietà collocano ElectionGuard all'interno del paradigma End-to-End Verifiable (E2E) che viene descritto nel Capitolo 4.3, con un forte riferimento alla trasparenza matematica e a strumenti di verifica pubblicabili a posteriori.

Il sistema utilizza principalmente questi strumenti crittografici :

- Cifratura omomorfica dei voti: ogni voto viene cifrato con una chiave pubblica, grazie alla crittografia omomorfica vista in precedenza è possibile sommare i voti cifrati, senza dover decifrare i singoli voti. In questo sistema vengono utilizzati schemi omomorfici basati su ElGamal.
- Prove crittografiche pubblicabili: viene generata una prova a conoscenza zero per ogni voto, per dimostrare la validità della scelta, senza doverne rivelare il contenuto.

Successivamente queste prove vengono pubblicate per poter essere verificabili da chiunque.

- Decifratura totale distribuita: la chiave privata utilizzata per la decifratura dei voti, come accade spesso, viene suddivisa tra più autorità elettorali, in modo tale che nessuna singola entità possa controllare o manipolare il risultato.

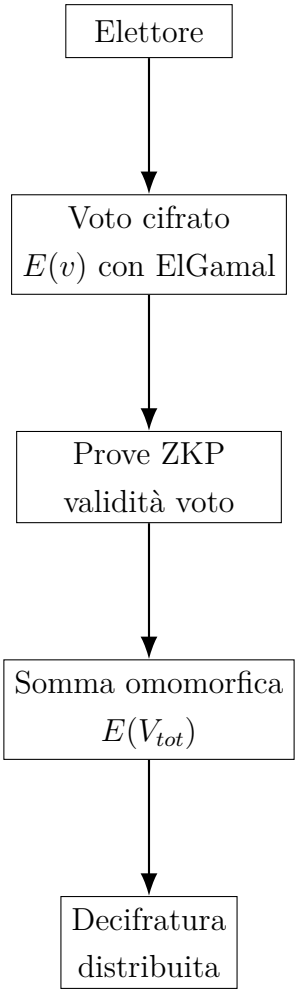

Figura 9: Schema semplificato di ElectionGuard.

5.5 Confronto tra i vari sistemi di voto elettronico analizzati

Ciascuno dei sistemi crittografici presentati precedentemente adotta metodi diversi per cercare di produrre un sistema di voto elettronico che garantisca correttezza, segretezza e verificabilità. Ogni sistema presenta vantaggi e limiti differenti.

Il sistema Estone rappresenta l'esempio più avanzato di voto elettronico, esso si basa su un'identità digitale molto forte e meccanismi che combinano firme digitali, crittografia asimmetrica e mix-nets. Nonostante ciò, ci vuole comunque una grande fiducia nel sistema digitale e ci sono tanti interrogativi riguardanti la sicurezza del dispositivo dell'elettore, che rimane una grande criticità.

La Svizzera ha un approccio più prudente ma i sistemi di voto vengono utilizzati solo in modo limitato. Uno dei modelli più recente è quello sviluppato da Swiss Post, si basano sulla crittografia omomorfica e prove a conoscenza zero. Il punto forte di questo sistema è che chiunque può verificare matematicamente la correttezza dello scrutinio. Il forte limite di questo approccio è che richiede una robusta complessità tecnica e un elevato costo computazionale.

Il Brasile utilizza un approccio radicalmente diverso, attraverso le urne elettroniche che vengono fisicamente isolate dalla rete durante la votazione, il che predispone una forte sicurezza. Il sistema come abbiamo visto si basa su firme digitali, controlli durante la procedura e controlli successivi. Il grande difetto di questo sistema è che non permette all'elettore o a terze parti di controllare che il proprio voto sia stato conteggiato correttamente.

Infine per quanto riguarda gli Stati Uniti non esiste un sistema di voto elettronico, in questo capitolo viene analizzato ElectionGuard, che è un'iniziativa che ha come obiettivo di introdurre verificabilità all'interno dei sistemi di voto tradizionali. Il vantaggio di questa iniziativa sarebbe quello di integrare la crittografia senza stravolgere infrastrutture o metodi di voto, mentre il limite è che, come abbiamo già detto, è un'iniziativa e non esiste uno standard a livello nazionale.

Nel complesso possiamo vedere che non esiste un modello ideale. Le varie differenze dimostrano che la progettazione di un sistema di voto digitale non è solo una questione tecnica ma anche culturale e istituzionale.

6 Casi di studio

Nel capitolo precedente ho analizzato come i diversi paesi hanno adottato i sistemi di voto elettronico. Per comprendere meglio i dettagli tecnici crittografici, in questo capitolo analizzerò protocolli e sistemi concreti su cui alcune realizzazioni politiche si fondano.

All'interno di questo capitolo ho selezionato alcuni casi di studio di sistemi di voto elettronico avanzati, che non vengono adottati in elezioni politiche ma vengono utilizzati in ambienti reali come esperimenti accademici o elezioni interne. Questi sistemi rappresentano dei modelli tecnici di riferimento e sono degli esempi su come dei fondamenti crittografici presentati precedentemente vengano messi in pratica.

6.1 Helios

Helios è uno dei sistemi di voto elettronico end-to-end verificali più noti nella letteratura accademica. Si tratta di una piattaforma open-source disponibile sul web che permette di realizzare votazioni in cui sia l'elettore che osservatori esterni possano verificare attraverso meccanismi crittografici che i voti siano stati conteggiati correttamente. [Wik26f]

Helios da la possibilità agli utenti registrati di creare delle elezioni. Ogni account è dotato di email, password ed ha la possibilità di creare un'elezione specificando nome e tempistiche. Una volta creata l'elezione Helios fornisce una chiave pubblica all'amministratore. L'amministratore prepara la scheda elettorale e aggiunge gli elettori che possono essere modificati fino all'inizio delle votazioni. Ogni elettore presente nella lista elettorale creata dall'amministratore riceve un'email con nome utente e password per quella specifica elezione, un'URL per la cabina elettorale e un hash dei parametri elettorali. L'elettore entrando nel link dell'email inizia il processo di voto. Una volta che l'elettore ha scelto le sue preferenze sigilla la scheda e fa attivare Helios per crittografarla e visualizza un testo cifrato. A questo punto il voto non è ancora stato registrato, l'elettore ha ancora la possibilità di modificarlo o confermare il voto. Una volta inviato il voto la scheda elettorale viene scartata per evitare che esista una prova diretta di cosa l'elettore ha votato. [Wik26f]

Figura 10: Flusso semplificato del processo di votazione in Helios.

Una volta capito il funzionamento generale di helios, successivamente proverò a spiegare come attraverso la crittografia vengono effettuati questi passaggi. Helios è un sistema di voto elettronico end-to-end verificable che si basa sulla crittografia asimmetrica, crittografia omomorfica e prove a conoscenza zero per garantire segretezza del voto, verificabilità pubblica e resistenza alla coercizione.

All'inizio dell'elezione, l'amministratore genera una coppia di chiavi crittografiche secondo lo schema di ElGamal, che si basa su un gruppo ciclico G, ovvero un insieme di numeri su cui è definita un'operazione di moltiplicazione modulare, generato da un elemento g, che consente di ottenere tutti gli altri elementi del gruppo. La chiave pubblica è definita come:

$$y = g^x \bmod q$$

dove x rappresenta la chiave privata principale. La chiave privata principale x non è detenuta da un singolo soggetto, ma viene suddivisa tra n persone. In particolare, la chiave è rappresentata come la somma di n valori segreti:

$$x = x_1 + x_2 + \cdots + x_n \pmod{q}$$

dove ciascun valore x_i è noto esclusivamente alla persona corrispondente.

L'elettore sceglie l'opzione m e genera un numero casuale $r \in \mathbb{Z}_q$. Il numero r è un segreto scelto dall'elettore, diverso per ogni votazione, e serve a mascherare il voto durante la cifratura.

Il voto viene trasformato in un voto cifrato

$$c = (c_1, c_2)$$

dove

$$c_1 = g^r, \quad c_2 = m \cdot y^r$$

Il voto cifrato $c = (c_1, c_2)$ viene successivamente accompagnato da una prova a conoscenza zero (ZKP). Questa prova, come abbiamo visto precedentemente, permette di dimostrare che il voto scelto dall'elettore è valido, senza mai rivelarne il contenuto reale.

In pratica, possiamo vedere le ZKP come un timbro di validità, in cui è possibile verificare che il voto è stato cifrato correttamente e che rientri nelle scelte possibili. Nessuno, neanche l'amministratore, può conoscere il voto effettivo.

Formalmente, la prova può essere rappresentata come:

$$\pi = \text{ZKP}\left\{ r : c_1 = g^r \ \wedge \ \frac{c_2}{g^m} = y^r \right\},$$

Il voto cifrato c e la prova π sono firmati con la chiave privata dell'elettore sk_v:

$$\sigma = \text{Sign}_{sk_v}(c, \pi)$$

dove σ rappresenta la firma digitale che garantisce l'autenticità del voto.

Successivamente il server verifica la firma e pubblica il voto cifrato sulla bacheca, in cui tutti i voti possono essere visualizzati e controllati da chiunque.

Attraverso la critttografia omomorfica, sommiamo tutti i voti cifrati, ovvero calcolando la moltiplicazione delle coppie cifrate:

$$c_{\text{agg}} = \prod_{i=1}^{N} c_i = \left(\prod_{i=1}^{N} g^{r_i}, \ \prod_{i=1}^{N} m_i \cdot y^{r_i} \right)$$

La moltiplicazione dei primi elementi c_1 dà:

$$\prod_{i=1}^{N} g^{r_i} = g^{r_1} \cdot g^{r_2} \cdot \cdots \cdot g^{r_N} = g^R, \quad R = \sum_{i=1}^{N} r_i$$

La moltiplicazione dei secondi elementi c_2 dà:

$$\prod_{i=1}^{N} m_i \cdot y^{r_i} = (m_1 \cdot m_2 \cdot \cdots \cdot m_N) \cdot y^{r_1+r_2+\cdots+r_N} = M \cdot y^R$$

Come abbiamo visto la chiave privata viene divisa in persone fidate che detengono piccole parti. Ogni sengola persona calcola la decriptazione parziale:

$$d_i = c_1^{x_i} = (g^R)^{x_i} = g^{Rx_i}$$

in cui:

- c_1 è la prima componente del voto aggregato cifrato $c_{\text{agg}} = (c_1, c_2)$;
- x_i è la porzione della chiave privata principale x posseduta dalla persona i;
- g è il generatore del gruppo utilizzato nella cifratura ElGamal;
- $R = \sum_{i=1}^{N} r_i$ è la somma dei numeri casuali scelti da ogni elettore per la cifratura dei propri voti.

La decrittazione finale restituisce il voto aggregato M combinando le decrittazioni parziali delle persone fidate che posseggono una parte della chiave privata:

$$M = \frac{c_2}{\prod_{i=1}^{n} d_i} = \frac{M \cdot y^R}{\prod_{i=1}^{n} g^{Rx_i}} = M$$

in cui:

- c_2 è la seconda componente del voto aggregato cifrato $c_{\text{agg}} = (c_1, c_2)$;
- d_i è la decrittazione parziale calcolata dalla persona i, $d_i = c_1^{x_i} = g^{Rx_i}$;

In questo modo si ottiene il voto aggregato M senza mai rivelare i singoli voti.

Successivamente ho inserito una tabella per sintetizzare quali fondamenti critttografici riescono a far si che il sistema soddisfi determinate proprietà.

Proprietà	**Meccanismo in Helios**
Segretezza	ElGamal + decrittazione distribuita
Integrità	Firma digitale dell'elettore
Verificabilità individuale	Ricevuta + ZKP
Verificabilità universale	Bacheca pubblica + ZKP
Resistenza alla coercizione	Scarto della scheda, voto cifrato

Tabella 1: Proprietà di sicurezza e i meccanismi corrispondenti in Helios

Infine possiamo dire che Helios rappresenta un modello operativo concreto di voto elettronico crittografico, che mostra come le primitive studiate nei capitoli precedenti possano essere integrate in un sistema reale, garantendo privacy, verificabilità e sicurezza pur rimanendo accessibile e trasparente agli elettori e agli osservatori esterni. [Int10; Hel11; Hel15]

6.2 Prêt à Voter / Scantegrity / Punchscan

Prêt à Voter, Scantegrity e Punchscan rappresentano una famiglia di sistemi di voto elettronico End-to-End verificabili che si distinguono da Helios perchè utilizzano supporti cartacei, essendo stati progettati principalmente per votazioni in presenza cercando di integrare alla trasparenza del voto tradizionale le garanzie crittografiche dei sistemi elettronici.

Prêt à Voter

Il sistema di voto End-to-End denominato Prêt à Voter è stato ideato da Peter Ryan dell'Università di Lussemburgo. Con l'obiettivo di garantire l'accuratezza del conteggio, dovuta alla massima trasparenza del processo, mantenendo comunque la massima privacy del voto. L'idea chiave di questo approccio è codificare il voto utilizzando l'elenco dei candidati randomizzati. In pratica, per esempio, supponiamo che l'elettore, che chiameremo Anne, si presenti al seggio elettorale. Anne sceglie casualmente una scheda di voto sigillata all'interno di una busta. La scheda contiene l'elenco in ordine casuale dei candidati e un codice casuale univoco. All'interno della cabina elettorale, Anne esprime il proprio voto nel modo tradizionale, apponendo una croce accanto al candidato prescelto. Dopo aver votato, la scheda viene separata in due parti: la parte sinistra, che contiene l'elenco dei candidati in ordine casuale, viene immediatamente scartata, mentre la parte destra, che riporta solo la posizione del segno di voto e il codice casuale, rimane all'elettore come ricevuta. Anna esce quindi dalla cabina con la sua ricevuta e si registra presso un funzionario elettorale, inserendo la ricevuta in un dispositivo. Il dispositivo registra il codice casuale e la posizione del voto, senza conoscere il nome del candidato scelto. La ricevuta cartacea viene firmata digitalmente e restituita all'elettore. [Wik]

L'ordine dei candidati sulla scheda è determinato da una permutazione casuale che indicheremo con π. L'elettore seleziona il candidato desiderato v, ma il voto pubblicato non è il nome del candidato bensì la sua posizione nella permutazione:

$$c = \pi(v)$$

dove:

- v è la scelta dell'elettore,

- $\pi(v)$ è l'indice della scelta nella permutazione π,
- c è il voto pubblicato.

In poche parole c è un numero che corrisponde alla posizione del candidato in quella scheda. Per dimostrare che l'ordine della scheda è onesto e non modificato successivamente viene vincolato con un commitment.

$$\mathrm{Com}(\pi) = g^{\pi} \cdot h^{r}$$

dove:

- r è un valore casuale scelto per garantire la permutazione non venga modificata in seguito e segretezza della scelta,
- g e h sono strumenti matematici forniti dal sistema utilizzati per "sigillare" l'informazione, ma non contengono informazioni di per sè.

Lo scrutinio avviene tramite una serie di mix-net, che hanno il compito di rimescolare e decifrare i voti. Per garantire il corretto rimescolamento vengono prodotte delle prove a conoscenza zero.

$$\mathrm{ZKP}\{\text{shuffle corretto}\}$$

Tramite ciò:

- l'elettore può verificare che sia presente il proprio voto,
- viene cancellato qualsiasi collegamento tra il voto e l'elettore,
- riusciamo a preservare la segretezza del voto.

Scantegrity

Scantegrity è un'estensione di Prêt à Voter, in cui a ogni candidato viene associato un codice segreto che viene stampato con inchiostro invisibile sulla scheda e rivelato solo quando l'elettore la marca. In pratica, scantegrity funziona come una normale scheda elettorale cartacea letta da uno scanner ottico.[Wik25]

In ogni scheda elettorale, accanto a ogni candidato, c'è un codice segreto, stampato però con inchiostro invisibile, in maniera tale che ad occhio nudo non sia visibile. L'elettore vota normalmente mettendo una X accanto alla preferenza, utilizzando però una penna apposita che rende visibile l'inchiostro invisibile. Una volta segnata la casella, appare un codice di conferma (es : "X7F9"); questo codice non indica la preferenza, ma solo che questo voto esiste. Infine se vuole l'elettore può scriversi il codice con il numero della scheda e verificare in seguito che il proprio voto sia stato conteggiato correttamente. Dopo

la fine delle elezioni, tutti i voti vengono pubblicati online insieme ai codici di conferma, così l'elettore può verificare che il suo voto sia stato conteggiato correttamente. [Wik25]

Possiamo dire che i codici sono sicuri perchè i codici vengono assegnati casualmente e non indicano la preferenza scelta. Non solo i codici prima del voto vengono "sigillati" e affidati a più soggetti indipendenti, per impedire che i codici vengano cambiati successivamente e per evitare che vengano stampate schede false. Infine, alla conclusione di ogni votazione, vengono rivelati tutti i codici della scheda e vengono confrontati con quelli "sigillati" in precedenza e se coincidono si ha la prova che le schede sono state stampate correttamente. [Wik25]

Tramite la crittografia spiegata negli scorsi capitoli possiamo dimostrare questo metodo in questo modo: [Cha+08]

Sia c_i il codice di conferma associato al candidato i e sia r_i un valore segreto scelto in modo casuale. Ogni codice di conferma viene vincolato tramite un *commitment* crittografico, calcolato come:

$$\mathrm{Com}(c_i) = H(c_i \parallel r_i)$$

dove $H(\cdot)$ è una funzione hash crittografica e il simbolo $\parallel$ indica la concatenazione tra il codice di conferma e il numero casuale r. Come abbiamo visto, il commitment consente di rendere pubblico un valore che dimostra l'esistenza del codice senza rivelarne il contenuto, garantendo che esso non possa essere modificato successivamente.

Dopo la fase di votazione: l'elettore conserva il codice di conferma c_i come ricevuta del proprio voto, successivamente il sistema pubblica l'elenco di tutti i codici di conferma corrispondenti ai voti validi in modo tale che chiunque può verificare che un determinato codice di conferma sia presente tra quelli pubblicati.

La sicurezza del sistema si basa sulle proprietà della funzione hash. In particolare, aventi due candidati distinti i, j, vale che:

$$H(c_i \parallel r_i) \neq H(c_j \parallel r_j)$$

Facendo ciò rende impossibile avere delle collisioni o la possibilità che un codice sostituisca un'altro. In questo modo, se ci sono delle alterazioni o modifiche dei voti o delle schede elettorali sarebbe facile rilevarle.

Infine possiamo dire che Scantegrity garantisce:

- **verificabilità individuale**, perchè ogni elettore ha la possibilità di controllare la presenza del proprio voto nel conteggio finale;
- **verificabilità universale**, data dalla possibilità degli osservatori esterni di verificare la correttezza del sistema e del risultato finale;

- **compatibilità con controlli cartacei**, grazie al fatto che maniene una scheda fisica riconteggiabile come nei sistemi elettorali tradizionali.

Il sistema Scantegrity II, non è solo toerico ma è stato utilizzato in un'elezione reale durante le elezioni municipali di Takoma Park nel 2009, rappresentando il primo esempio di applicazione di un sistema di voto end-to-end verificabile in un contesto elettorale governativo con tutela della segretezza del voto [CCC+10].

Punchscan

Punchscan è molto simile a Prêt à Voter ma utilizza una scheda composta da due fogli separati, ciascuno dei quali da solo non rileva il voto espresso dall'elettore.

Una scheda elettorale Punchscan è formata da due strati di carta, uno posto superiormente e uno inferiormente. Nello strato superiore sono inseriti i nomi dei candidati e un simbolo o una lettera accanto a ciascun nome e in fondo dei fori rotondi. Nello strato inferiore ci sono dei simboli corrispondenti ai simboli accanto ai candidati visibili dai fori dello strato superiore. L'elettore deve individuare il foro con il simbolo del candidato prescelto e segna il foro con un pennarello che è più grande del buco. Successivamente divide la scheda in due parti e sceglie uno strato da conservare come ricevuta e distrugge l'altro. Lo strato che l'elettore conserva viene scansionato al seggio per il conteggio dei voti. Risulta importante sapere che l'ordine dei simboli viene generato casualmente, quindi è diverso per ogni scheda, e nessuno può collegare la ricevuta al voto effettivo. [Wik26j]

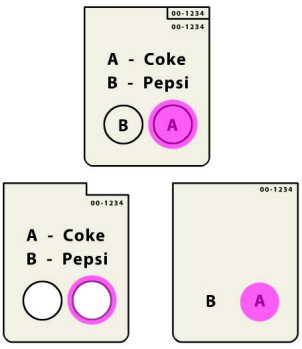

Figura 11: Scheda elettorale Punchscan [Wik26j]

In Punchscan, possiamo vedere il voto v come la combinazione di due parti:

$$v = s_1 \oplus s_2,$$

dove:

- s_1 è l'informazione contenuta nel primo foglio,
- s_2 è l'informazione contenuta nel secondo foglio.

Ogni parte viene ”sigillata” tramite un commitment crittografico. In parole semplici come abbiamo visto, si crea una sorta di “busta digitale” che permette di verificare successivamente il contenuto senza rivelarlo prima del momento opportuno:

$$\mathrm{Com}(s_1), \quad \mathrm{Com}(s_2)$$

Solo combinando entrambe le parti s_1 e s_2 è possibile ricostruire il voto v. [Bit26]
Dal punto di vista crittografico, Punchscan garantisce:

- **Privacy**: nessuno può determinare il voto osservando una sola parte della scheda;
- **Integrità**: i voti non possono essere modificati dopo la registrazione, grazie ai commitment;
- **Receipt-freeness**: l'elettore non può dimostrare il voto anche conservando uno dei due fogli.

7 Sicurezza del Client Votante e del Dispositivo dell'Elettore

In un sistema di voto elettronico, la sicurezza non riguarda solo i protocolli crittografici visti in precedenza, in cui si cerca di proteggere la segretezza del voto e l'integrità delle votazioni, ma riguarda anche la protezione del client votante, ovvero il PC, lo smartphone, il tablet o il terminale dedicato con cui l'elettore esprime il proprio voto. In questo capitolo analizzerò le possibili vulnerabilità del client di voto, i rischi e le varie contromisure crittografiche applicabili.

Il terminale dell'elettore (client) tramite cui l'elettore vota è il primo punto di accesso al sistema di voto, ma paradossalmente è anche il punto più vulnerabile. Nel caso di sistemi di i-voting, ovvero votazione con l'utilizzo di internet in cui si utilizza un dispositivo personale, il dispositivo non è sotto il controllo diretto dell'autorità elettorale e può essere soggetto a malware, phishing (truffe informatiche in cui i malintenzionati inviano email, sms o messaggi falsi mascherati da enti legittimi), configurazioni non sicure o software obsoleti. Questa vulnerabilità è molto rilevante e problematica nel sistema di voto, perchè se il sistema è compromesso già prima che l'elettore voti, si potrebbe intercettare o manipolare la preferenza dell'elettore prima che entri nel sistema e nel protocollo crittografico. [Cal21]

Le principali vulnerabilità del dispositivo di voto sono:

- **Malware**: un malware già installato sul dispositivo può modificare la preferenza o addirittura rubare le credenziali private dell'elettore;

- **Phishing**: come accennato prima tecniche in cui tramite email o sms fasulli è possibile ingannare l'elettore per rubare le credenziali;
- **Analisi del traffico crittografato**: anche se il dato viene trasmesso in forma crittografata è possibile analizzare informazioni come tempi di invio o dimesioni dei paccchetti per dedurre informazioni sul voto o sull'elettore. Questo attacco è anche noto come "inference attack su traffico criptato";
- **Problemi con l'autenticazione o gestione delle chiavi**: l'affidabilità del sistema crittografico dipende anche dall'elettore e si basa sul fatto che esso protegga le proprie chiavi private e le credenziali. Se vengono salvate o gestite in maniena non adeguadata, tutto sistema di voto può essere facilmente compromesso.

[McA25]

Per riuscire a contrastare le vulnerabilità, viste in precedenza, legate al dispositivo dell'elettore bisogna procedere ad un approccio su più livelli:

- **Utilizzo di ambienti sicuri o dispositivi dedicati**: per evitare l'espositzione del sistema ad un software non sicuro, alcuni sistemi adottano o dispositivi di voto dedicati, oppure si basano su ambienti che vengono chiamati trusted execution environments (TEE). In questi ambienti il voto viene generato e cifrato in modo isolato dal resto del sistema operativo;
- **Autenticazione forte e hardware security**: Un'autenticazione forte, come per esempio un autenticazione a più fattori può verificare in maniera più affidabile l'identità dell'elettore. Questa autenticazione può essere affiancata da dispositivi harware di sicurezza come per esempio HSM o i token crittografici, in cui il livello di protezione e controllo aumenta ulteriormente. Questi dispositivi hardware di sicurezza sono oggetti fisici progettati per proteggere informazioni, in particolare chiavi crittografiche, che servono per esempio per autenticarsi o firmare. Questi dispositivi servono perchè le chiavi non vengono mai salvate o usate all'interno del computer, ma rimangono all'interno di questi dispositivi.;
- **Protezione del software client**: Il software client, ovvero il software utilizzato dall'elettore per votare, è importante assicurarsi che il programma sia stato modificato o compromesso da terzi. Tecniche come code signing (firma del codice), in cui il software viene firmato digitalmente dallo sviluppatore, serve per garantire autenticità e integrità del software perchè in caso in cui essso fosse stato modificato la firma non risulta più valida. Oppure effettuare numerosi aggiornamenti automatici, per correggere possibili vulnerabilità e sostituire versioni vecchie e compromesse, riduce il rischio che l'utente usi un software non sicuro. Infine la verifica di integrità in cui

prima dell'uso il software controlla che non sia stato alterato o non corrisponda alla versione ufficiale, aiuta a garantire che il client non sia stato manomesso;

- **Formazione e comportamento sicuro dell'elettore**: Molto importante e da non sottovalutare è anche la consapevolezza del votante sulle minacce, come la verifica che si stia collegando al sito ufficiale, la gestione sicura di credenziali, o l'uso di antivirus aggiornati, è una componente fondamentale della sicurezza complessiva.

[Pia26b]

Nonostante noi possiamo applicare le migliori pratiche possibili restano dei limiti a qualsiasi sistema che consenta il voto da un hardware non controllato. In contesti reali come un elezione politica, una compromissione del client può compromettere gravemente tutto il sistema di voto. Per questo motivo, molte giurisdizioni preferiscono l'uso di terminali dedicati sotto la supervisione fisica dell'autorità elettorale. [Cal21]

Come abbiamo visto nei capitoli precedenti, possiamo dire che tramite la crittografia nei protocolli di voto possiamo garantire segretezza, integrità e verificabilità dei voti. Invece la sicurezza del client votante resta una questione critica e molto discussa. In sintesi, per proteggere l'intero processo di voto sono necessari non solo algoritmi crittografici avanzati, ma anche misure di sicurezza del client.

8 Usabilità, accessibilità e fattore umano

Come abbiamo visto, quando si progettano sistemi di voto elettronico la sicurezza crittografica non è l'unico punto fondamentale da tenere in considerazione, vedremo che anche l'usabilità, l'accessibilità e il fattore umano hanno un ruolo fondamentale. Per esempio, un sistema robusto dal punto di vista crittografico, ma difficile da usare o non accessibile a tutti, può compromettere tutta la votazione.

In seguito, provo a definire cosa si intende per questi termini:

- **Usabilità**: Con questo termine si intende con quanta facilità ed efficienza può essere utilizzato il sistema dagli elettori per esprimere il voto. Può comprendere aspetti come: chiarezza dell'interfaccia, facilità di navigazione e feedback comprensibile durante la votazione;

- **Accessibilità**: Con questo termine si intende quanto il sistema sia accessibile a tutti, anche a persone per esempio con disabilità visive, motorie o uditive.;

- **Fattore umano**: Con fattore umano si intendono tutti gli aspetti psicologici e cognitivi dovuti all'interfaccia utente, bisogna evitare il più possibile l'errore umano da parte degli elettori.

[Nat22; SEC26]

Questi tre fattori vedremo che sono fondamentali in un sistema di voto elettronico, perchè un sistema sicuro ma difficile da usare può portare l'elettore a commettere errori e a non fidarsi dei risultati.

I protocolli crittografici, a volte così complicati, sono difficili da spiegare e rendere intuitivi all'utente finale. Se un elettore non riesce a capire bene come funziona il processo o se il suo voto è stato conteggiato correttamente, perde la fiducia nel sistema. Alcune ricerche mostrano che nella progettazione di un sistema bisogna tenere conto anche di alcuni aspetti come : Feedback visivo e chiaro su ogni fase del voto, rendere l'interfaccia utente più minimalista e semplice possibile evitando numerosi passaggi o istruzioni ambigue. Infine molto importante se possibile aggiungere test di usabilità con utenti reali per avere riscontri su possibili punti di confusione. [Nat22]

L'accessibilità invece, al giorno d'oggi è un requisito obbligatorio all'interno di ogni sistema. Esistono standard di accessibilità come le WCAG (Web Content Accessibility Guidelines), che sono delle linee guida a livello internazionale per l'accessibilità dei contenuti all'interno del web. Queste linee guida si basano su quattro principi: percepibilità, utilizzabilità, comprensibilità e robustezza, suddivisi in tre livelli di conformità (A, AA, AAA). E' molto importante che tutti gli strumenti di assistenza, come per esempio screen reader, il controllo vocale o tastiere alternative siano compatibili con il software di voto, in modo tale da garantire la possibilità di voto a tutti senza escludere nessuno. Questo aspetto dell'accessibilità è molto importante proprio per questo, soprattutto nei sistemi di voto, per il principio costituzionale di suffragio universale, in cui nessun elettore deve essere escluso. [Acc21; Uni26; Nat22]

La sicurezza non riguarda solo le abilità tecniche implementate nel sistema, ma come abbiamo detto precedentemente, comprende anche la percezione dell'utente, è molto importante far capire anche a un utente non esperti perchè un sistema è affidabile se no può ricadere negativamente nella fiducia che ha un elettore sul sistema.

Alcuni fattori umani che devono essere inclusi e controllati all'interno di un sistema possono essere:

- **Comprensione del processo**: bisogna all'interno della progettazione tenere conto che molti elettori non sono esperti e non hanno competenze di sicurezza informatica, quindi è necessario che anche loro possano comprendere e successivamente valutare autonomamente se il sistema e il protocollo crittografico lo ritengono affidabile;

- **Feedback e trasparenza delle operazioni**: delle interfacce che mostrano la conferma del voto o prove che confermano l'avvenuta votazione senza rivelare il voto possono aumentare la fiducia dell'utente nel sistema;

- **Errori o doppie votazioni**: è importante che il sistema tenga conto che l'elettore possa effettuare degli errori. Se l'elettore per esempio sbaglia a votare e non sa

come correggerlo o un sistema in generale troppo complicato, può creare frustazione e ridurre la partecipazione al voto. Il protocollo crittografico, in generale il sistema deve prevedere questi tipi di errori e gestirli in maniera adeguata.

[SEC26; Nat22]

Un tema ricorrente nei sistemi crittografici su cui ancora oggi si parla molto nell'ambito della ricerca è il compromesso tra sicurezza e usabilità. Maggiore sicurezza crittografica come l'utilizzo di prove a conoscenza zero o mix-nets o l'autenticazione a più fattori, introduce complessità e crea un sistema molto più complesso da utilizzare soprattutto per utenti che non sono esperti nell'ambito. Invece rendere un sistema facile da utilizzare, rapido e comprensibile a tutti può indebolire alcune garanzie di sicurezza. Creare un sistema che trovi il giusto compromesso tra questi due aspetti, non è sempre facile ma necessario per avere un sistema completo.

In conclusione un sistema di voto che utilizza la crittografia avanzata, non basta, è necessario tenere in considerazione anche usabilità, accessibilità e fattore umano se no anche il sistema più sicuro può risultare inefficace alla pratica. Per tanto quando si progetta e si implementa un sistema di voto elettronico bisogna includere:

- **Test di usabilità e accessibilità con utenti reali**
- **Adottare standard e linee guida di accessibilità**
- **Utilizzare interfacce intuitive con feedback chiaro e comprensibile**
- **Sensibilizzare e formare gli elettori**.

Tramite queste piccole implementazioni possiamo garantire non solo una sicurezza crittografica, ma anche una qualità reale nell'esperienza di voto. [Nat22; Uni26]

9 Simulazione di Attacco a un Sistema di Voto Crittografico Semplificato

In questo capitolo presenterò una simulazione controllata di un attacco a un sistema di voto elettronico, con l'obiettivo di mettere in evidenza quali proprietà crittografiche proteggono il voto e in quali punti un attaccante potrebbe intervenire e interferire con il sistema se queste proprietà non sono implementate.

Per questo capitolo prendo in considerazione il sistema Helios che abbiamo visto nel capitolo dei casi di studio. Un sistema Helios è composto dai seguenti fattori:

- Elettore
- Client di voto

- Server elettorale
- Autorità di scrutinio

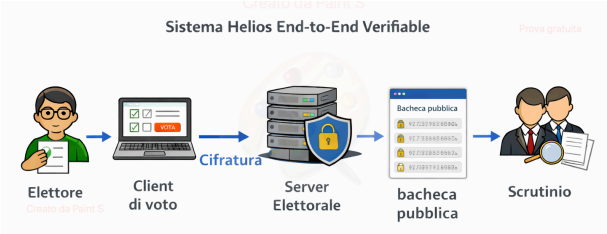

Figura 12: Rappresentazione grafica semplificata del sistema Helios

Come possiamo vedere anche dall'immagine il flusso del voto avviene in questo modo:

- L'elettore all'interno del proprio dispositivo seleziona la propria preferenza,
- il voto viene cifrato sul client,
- il voto cifrato viene inviato al server,
- i voti cifrati vengono pubblicati su una bacheca pubblica,
- infine avviene lo scrutinio tramite crittografia omomorfica.

All'interno del sistema Helios viene utilizzato l'algoritmo asimmetrico di cifratura Elgamal, che ho spiegato approfonditamente nel capitolo 3.1. Viene utilizzato questo algoritmo perchè possiede due proprietà fondamentali: la sicurezza semantica, ovvero se qualcuno intercetta il voto cifrato è praticamente impossibile capire quale sia o decifrarlo, e omomorfismo applicativo, ovvero si possono combinare i voti senza decifrarli. È importante sottolineare che un algoritmo in teoria sicuro non garantisce sicurezza nel suo complesso. Nella realtà, nei sistemi di voto elettronici basati su ElGamal, sono stati infatti riscontrati dei problemi, come l'utilizzo di chiavi crittografiche di dimensioni troppo piccole come per esempio in Russia. [Wir19]

ElGamal ha bisogno di alcuni elementi matematici per funzionare, possiamo immaginarli come "ingredienti della ricetta".

- Un gruppo ciclico G: un insieme di numeri su cui facciamo i calcoli che può essere generato a partire da un solo elemento.
- Generatore g: l'elemento a partire da cui si può generare il groppo. Ovvero se lo combini con se stesso tante volte usando l'operazione del gruppo, riesci a ottenere tutti gli altri elementi del gruppo.
- Il numero di elementi del gruppo G è un numero primo q.

Si sceglie la chiave privata x, prendendo un grande numero intero casuale x che si trova tra 1 e $q-1$. Questo numero deve essere veramente casuale e segreto, perché chi lo scopre può decifrare tutti i voti.

Una volta scelto x, si calcola la chiave pubblica:

$$h = g^x$$

Noi abbiamo il voto v, che viene codificato numericamente tramite l'esponenziale

$$g^v.$$

In questo modo il voto viene trasformato in un elemento del gruppo ciclico G, poiché g è un generatore di G e ogni sua potenza appartiene al gruppo. Una volta trasformato il voto in numero, possiamo crittografare le informazioni, il client generando un valore casuale r, fondamentale per garantire la sicurezza della cifratura, calcola:

$$\begin{cases} c_1 = g^r \\ c_2 = h^r \cdot g^v \end{cases}$$

Il voto cifrato è quindi rappresentato dalla coppia:

$$C = (c_1, c_2)$$

Successivamente possiamo vedere come la preferenza dell'elettore v, all'interno del dispositivo dell'elettore tramite la cifratura ElGamal si trasforma in c1 e c2, ora il dispositivo può trasmettere il risultato al server centrale.

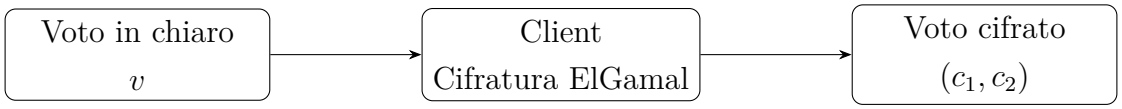

Figura 13: Trasformazione del voto in chiaro in voto cifrato mediante ElGamal

Una volta cifrato il messaggio, simuliamo un attaccante che mira a modificare il voto, ovviamente cercando di mantenere la validità del messaggio, onde evitare che venga scoperto.

A questo punto, se noi simulassimo un attacco in un sistema privo dello strumento: "Prove a conoscenza zero" (citate nel capitolo 3.5).

L'attaccante intercetta il voto cifrato che è della forma:

$$C = (c_1, c_2)$$

e modifica il secondo componente c_2 moltiplicandolo per il generatore g:

$$c_2' = c_2 \cdot g$$

Possiamo osservare che il generatore g è un parametro pubblico del sistema ElGamal. Di conseguenza, anche un attaccante è in grado di utilizzarlo per modificare il voto cifrato senza conoscere né il voto originale né la chiave privata. Quindi il nuovo voto cifrato risulta:

$$C' = (c_1, c_2')$$

Una volta modificato il messaggio e inviato al server centrale, grazie alla proprietà omomorfica di ElGamal i voti vengono sommati tra loro e poi solo successivamente decifrati. Possiamo calcolare il cifrato del totale dei voti come prodotto dei cifrati singoli:

$$C'_{\text{tot}} = \left(\prod_{i=1}^{n} c_{1,i},\ c_2' \cdot \prod_{j \neq i} c_{2,j} \right) = \left(g^{\sum_i r_i}, g^{(\sum_i v_i)+1} h^{\sum_i r_i} \right)$$

Se non avessimo modificato $c2'$ avremmo la decifratura del totale in questa forma:

$$\text{totale decifrato} = \frac{\prod_i c_{2,i}}{(\prod_i c_{1,i})^x} = g^{\sum_i v_i}$$

Invece con la modifica di $c2'$ possiamo vedere il totale decifrato in questa forma:

$$\text{totale decifrato modificato} = \frac{\prod_i c'_{2,i}}{(\prod_i c_{1,i})^x} = g^{(\sum_i v_i)+1}$$

Si vede chiaramente che il totale dei voti risulta alterato di +1, pur restando formalmente valido appartenendo al gruppo G.

Fase	**Voto normale**	**Voto modificato**
Voto cifrato singolo	$C_i = (c_{1,i}, c_{2,i})$	$C'_i = (c_{1,i}, c'_2)$
Aggregazione totale	$C_{\text{tot}} = (\prod c_{1,i}, \prod c_{2,i})$	$C'_{\text{tot}} = (\prod c_{1,i}, c'_2 \cdot \prod_{j \neq i} c_{2,j})$
Decifratura finale	$g^{\sum_i v_i}$	$g^{(\sum_i v_i)+1}$

Per prevenire questo attacco possiamo utilizzare le prove a conoscenza zero o ZKP, che in questo caso servono a dimostrare che il voto è valido senza rivelare il contenuto del voto.

Per fare ciò è necessario l'utilizzo della seguente formula:

$$\frac{c_2}{h^r} = g^v$$

Il suo scopo principale è "isolare" la parte del voto puro g^v, eliminando la componente casuale h^r.

Solo dopo ciò e solo dopo che la formula ha dimostrato la veridicibilità del voto, il client fornisce una Zero-Knowledge Proof (ZKP) che dimostra la correttezza dell'operazione, mantenendo l'anonimato del voto.

Infine abbiamo ottenuto il risultato voluto cioè: il server può verificare che il voto sia valido senza conoscerne il contenuto. E' necessario specificare che questo è solo uno dei possibili scenari poichè le variabili cambiano a seconda degli strumenti e sistemi presi in esame. Un attacco alternativo potrebbe essere la compromissione del dispositivo dell'elettore prima della cifratura. In questo caso agendo prima della cifratura, la crittografia non può intervenire.

Per esempio l'elettore esprime il voto $v = 0$, un malware presente sul dispositivo modifica il valore in $v = 1$, senza che l'elettore se ne accorga. Il sistema riesce a cifrare correttamente il voto modificato. Il voto cifrato risulta quindi matematicamente valido, ma non rappresenta la reale intenzione dell'elettore.

$$\begin{array}{ccccc} \text{Utente} & & \text{Malware} & & \text{Cifratura} \\ 0 & \rightarrow & 1 & \rightarrow & Enc(1) \end{array}$$

Possiamo vedere che quest'attacco non viola il protocollo crittografico ElGamal, ma rovina comunque il sistema di voto.

Attraverso questa simulazione possiamo notare alcuni aspetti fondamentali della sicurezza del voto elettronico. Innanzitutto, la crittografia interviene solo dopo che il voto è stato inserito, quindi eventuali alterazioni effettuate prima della cifratura sfuggono alla protezione. Inoltre esistono proprietà crittografiche che garantiscono fiducia e sicurezza nel sistema di voto elettronico come in questo caso le prove a conoscenza zero.

10 Comparazione dei sistemi analizzati

In questo capitolo cercherò di mettere a paragone i principali paradigmi di voto elettronico analizzati nei capitoli precedenti. Analizzerò i sistemi di voto elettronico confrontandoli secondo i requisiti spiegati nel capitolo 2.

I sistemi basati sulle mix-net, grazie all'utilizzo di una sequenza di server crittografici che rimescolano e decifrano i voti, riescono a interrompere qualsiasi collegamento tra l'elettore e il voto espresso, garantendo così un elevato livello di anonimato. Infatti possiamo notare tra i principali vantaggi di questo sistema c'è un forte anonimato e un elevata solidità teorica. Invece come limiti principali abbiamo: una forte complessità computazionale, la difficoltà di un'implementazione corretta e il fatto che la verificabilità del sistema è comprensibile solo a utenti esperti.

I sistemi basati sulla crittografia omomorfica consentono di decifrare la somma di tutti i voti cifrati, evitando di decifrare i singoli voti. I principali vantaggi di questo sistema sono che lo scrutinio finale avviene direttamente sui dati cifrati e grazie a ciò abbiamo

una buona trasparenza nel conteggio. Come abbiamo visto nel capitolo precedente con il sistema di Helios, un forte limite è la necessità delle ”Prove a conoscenza zero” o ”Zero-Knowledge Proofs”.

I sistemi End-to-End Verifiable (E2E) si basano sul fatto che danno la possibilità all'elettore di verificare che il suo voto sia stato correttamente registrato e incluso nel conteggio, senza compromettere la segretezza del voto. Infatti garantisce un elevato livello di trasparenza e riduce la fiducia cieca nel sistema. Richiede però delle interazioni complesse per l'elettore con un forte rischio di errori umani.

Negli ultimi anni sono stati proposti sistemi di voto elettronico che si basano sulle blockchain, si caratterizzano perchè registrano i voti su un registro distribuito. Utilizzando un registro pubblico garantisce un elevata trasparenza, con il rischio di avere dei possibili problemi di privacy.

Sistema	**Vantaggi**	**Svantaggi**
Mix-nets	Forte anonimato; separazione crittografica tra identità dell'elettore e voto espresso	Elevata complessità computazionale; difficoltà di auditing e implementazione corretta
Sistemi omomorfici	Scrutinio effettuato su voti cifrati; buona scalabilità del conteggio	Limitata resistenza alla coercizione; necessità di prove crittografiche complesse

Sistema	**Vantaggi**	**Svantaggi**
Sistemi End-to-End Verifiable (E2E)	Trasparenza completa del processo elettorale; verificabilità individuale e universale	Usabilità ridotta per l'elettore; rischio di errori umani nelle fasi di verifica
Sistemi blockchain-based	Immutabilità dei dati; elevata auditabilità pubblica	Problemi di privacy; scarsa maturità tecnologica e limitata scalabilità

Possiamo vedere che nessun paradigma di voto elettronico è perfetto e soddisfa a pieno tutti i requisiti ideali. In base al contesto e alla situazione scegliamo il paradigma che più rispecchia i requisiti che vogliamo raggiungere dal sistema di voto. [Seq21; KHC22a; Eme25]

11 Aspetti pratici e normative

L'utilizzo di determinate tecnologie nei sistemi di voto elettronico non dipende solo dalla progettazione tecnica, ma deve inserirsi all'interno di un quadro normativo. In ambito internazionale esistono numerosi strumenti e standard che danno indicazioni su come organizzare e valutare il voto elettronico, in maniera tale che tuteli l'integrità, la segretezza, l'uguaglianza e la trasparenza del processo. Nonostante questa non sia una tesi improntata su un ambito legale o di norme, secondo me è importante conoscere le più importanti.

Il Consiglio d'Europa è stata la prima e l'unica organizzazione ad aver introdotto specifiche raccomandazioni sul voto elettronico. All'interno della REC(2014)11 vengono definiti i criteri legali, operativi e tecnici che il sistema di voto elettronico deve rispettare. Questo documento è stato un riferimento nazionale per standard di e-voting. [Eli25; Cou17b]

Nel 2017 è stata introdotta la CM/REC(2017)5, la nuova raccomandazione che aggiorna e amplia la REC(2014)11 a seguito dei progressi tecnologici e delle esperienze raccolte. Questa raccomandazione mira a garantire che i mezzi elettronici utilizzati all'interno del sistema di voto rispettino i principi di un elezione libera e segreta. Questa raccomandazione fornisce delle linee guida per far si che vengano rispettati i principi di democrabilità all'interno dell'e-voting. [Cou17a]

All'interno dell'OSCE, ovvero un'organizzazione per la sicurezza e la cooperazione in Europa, l'ODIHR, ovvero l'ufficio per le istituzioni democratiche e i diritti umani, ha elaborato degli strumenti pratici per l'osservazione e la valutazione delle tecnologie elettorali. Esiste un "Handbook for the Observation of New Voting Technologies", in cui si offre una guida per valutare le tecnologie utilizzate all'interno di un sistema di voto, per assicurarsi che rispettino la correttezza delle elezioni, incluse le macchine elettroniche di voto, gli scanner e i sistemi di voto via Internet. La funzione dell'ODIHR non è quella di "giudicare" le elezioni, perché questo in realtà spetta alle istituzioni nazionali di ciascun Paese e ai suoi cittadini. Tuttavia, l'osservazione garantisce un ulteriore livello di trasparenza, controllo e responsabilità pubblica. Negli ultimi anni, l'ODIHR ha pubblicato un nuovo manuale intitolato: "Handbook for the Observation of Information and Communication Technologies (ICT) in Elections", in cui analizza l'impatto complessivo delle tecnologie digitali all'interno del sistema di voto. [OSC13; OSC24; OSC26]

In sintesi, le linee guida del Consiglio d'Europa e le pubblicazioni dell'OSCE/ODIHR riescono a darci un quadro normativo completo per valutare e realizzare anche un sistema di voto elettronico. Esse non si limitano a definire criteri generali, ma offrono anche strumenti concreti per monitorare e analizzare l'impatto delle tecnologie elettorali nella pratica.

Le raccomandazioni del Consiglio d'Europa mettono in luce la necessità che il voto

elettronico sia trasparente e affidabile, infatti richiedono che l'elettore possa fidarsi del processo elettorale pur utilizzando tecnologie digitali. Questo fa si che i sistemi di e-voting debbano essere progettati in modo tale che tutte le fasi critiche che vanno dalla raccolta del voto al conteggio finale siano verificabili e non compromettano i diritti degli elettori. Le norme e gli standard internazionali riescono ad orientarci in maniera più concreta su come progettare un sistema di voto elettronico corretto.

Nel contesto della progettazione e valutazione dei sistemi di voto elettronico, oltre al quadro normativo che ho descritto in precedenza, esistono anche linee guida tecniche e criteri operativi proposti da comunità scientifiche specializzate. Un esempio significativo è rappresentato dalle raccomandazioni elaborate dalla International Association for Cryptologic Research (IACR), un'associazione internazionale di ricercatori in crittografia. L'IACR ha introdotto dei requisiti che costituiscono un insieme di best practice tecnologiche da considerare nella progettazione di sistemi di voto elettronico con una forte componente crittografica. È importante osservare che queste best practice non sono completi dal punto di vista legale o normativo per elezioni di Stato, sono stati pensati originariamente per la gestione di elezioni interne all'associazione e per criteri di sicurezza crittografica.

Questi documenti mettono in evidenza quanto sia neccessiario bilanciare l'innovazione con i requisiti legali e di fiducia pubblica, per evitare che la tecnologia comprometti la correttezza delle elezioni.

12 Conclusione

In questa tesi ho cercato di esplorare i fondamenti crittografici, i paradigmi tecnologici e gli aspetti normativi dei sistemi di voto elettronico. Sono partita dai requisiti chiave che sono necessari in un sistema di voto elettronico, come l'idoneità, verificabilità, la verificabilità universale, la ricevuta di voto e la resistenza alla coercizione. Sono passata all'analisi dei fondamenti crittografici come la crittografia asimmetrica, l'omomorfismo, firme digitali, schemi di commitment e prove a conoscenza zero, che mostrano come degli strumenti matematici vengano utilizzati e sono alla base determinati sistemi di voto elettronici. Successivamente ho analizzato i paradigmi dei sistemi di voto e spiegato il funzionamento di alcuni sistemi di voto, mettendo in comparazione i vari compromessi differenti che offrono, come privacy, verificabilità e praticità di implementazione. Ad esempio, le soluzioni E2E consentono trasparenza e verificabilità senza compromettere la segretezza del voto, mentre i sistemi basati su blockchain promettono decentralizzazione e immutabilità del registro dei voti, ma devono ancora affrontare sfide legate alla scalabilità e alla privacy. Prendendo anche in considerazione l'analisi delle implementazioni reali in diverse giurisdizioni, come Estonia, Brasile e Stati Uniti, evidenziando che, sebbene la teoria crittografica fornisca strumenti molto potenti, l'adozione pratica di tali sistemi

richiede anche un solido quadro normativo e di fiducia sociale, oltre a processi di implementazione e verifica trasparenti. Anche nel contesto svizzero, ad esempio, l'adozione di sistemi di voto elettronico coinvolge misure di sicurezza e revisioni periodiche per garantire la conformità alle aspettative di integrità e trasparenza. Ho presentato alcuni casi di studio come Helios, molto utilizzato e Prêt à Voter, Scantegrity, Punchscan. Sono stati introdotti anche temi molto importanti e molto discussi come la sicurezza del client votante e del dispositivo dell'elettore, usabilità, accessibilità e fattore umano, che non sono strettamente legati alla crittografia ma necessari per costituire un sistema di voto elettronico sicuro. Molto interessante seconto me è la simulazione di un attacco a un sistema di voto crittografico, in cui prendo in considerazione un sistema Helios che abbiamo visto nei capitoli precedenti e simulo a livello pratico crittografico e matematico il momento in cui un attaccante prova e riesce a cambiare il voto di un elettore. Secondo me questo capitolo è uno dei più interessanti perchè mette insieme tutti gli argomenti trattati in precedenza, come il sistema Helios o i requisiti di un sistema, come la crittografia asimmetrica, la crittografia omomorfica le prove a conoscenza zero, e molti altri argomenti. Questo capitolo è molto interessante anche perchè riesce a far capire meglio il funzionamento nella realtà di un sistema di voto elettronico. Infine negli ultimi capitoli tratto il tema del sistema di voto elettronico esplorandolo da un punto di vista normativo. In questa ricerca abbiamo visto come il tema di un sistema di voto elettronico sia in continua evoluzione e future soluzioni crittografiche potranno superare alcune limitazioni attuali, sperando di ampliare l'applicazione pratica del voto elettronico in contesti reali. In conclusione, il voto elettronico rappresenta un argomento promettente per l'evoluzione dei processi democratici, ma per l'adozione c'è bisogno di un forte equilibrio tra robustezza crittografica, normative adeguate, trasparenza procedurale e fiducia degli elettori. I progressi nella ricerca crittografica, uniti a un quadro normativo solido e a una valutazione continua delle tecnologie emergenti, possono permettere di affrontare le sfide rimanenti e di realizzare sistemi di voto che siano davvero sicuri, verificabili e accettabili per la società.

Bibliografia

[Acc21] AccessiWay. *WCAG: cos'è questa sigla, cosa sono le guidelines e come rispettarle*. 2021. URL: https://www.accessiway.com/it/blog/wcag-cose-questa-sigla-cosa-sono-le-guidelines-e-come-rispettarle.

[Bit26] BitcoinWiki. *Punchscan — Basic auditing procedures*. Accessed: 02-02-2026. 2026. URL: https://bitcoinwiki.org/wiki/punchscan#Basic_auditing_procedures.

[Cal21] Vincenzo Calabrò. *Voto elettronico: modalità attuative e misure tecniche per la sicurezza della web application*. Cybersecurity360. 2021. URL: https://www.cybersecurity360.it/cybersecurity-nazionale/voto-elettronico-modalita-attuative-e-misure-tecniche-per-la-sicurezza-della-web-application/#:~:text=Voto%20elettronico%3A%20modalit%C3%A0%20attuative%20e%20misure%20tecniche%20per%20la,il%20sistema%20garantisce%20che%20le%20informazioni%20sui%20votanti%20vengano.

[CCC+10] Richard Carback, David Chaum, Jeremy Clark et al. *Scantegrity II Municipal Election at Takoma Park: The First End-to-End Binding Governmental Election with Ballot Privacy*. 2010. URL: https://vote.caltech.edu/working-papers/96.

[Cha+08] David Chaum et al. *Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes*. 2008. URL: https://www.usenix.org/legacy/event/evt08/tech/full_papers/chaum/chaum_html/index.html?utm_source=chatgpt.com.

[Cha+24] David Chaum et al. *Votexx: Extreme Coercion Resistance*. 2024. URL: https://eprint.iacr.org/2024/1354.

[Cou17a] Council of Europe. *Council of Europe adopts new Recommendation on Standards for E-Voting*. 2017. URL: https://www.coe.int/en/web/portal/-/council-of-europe-adopts-new-recommendation-on-standards-for-e-voting.

[Cou17b] Council of Europe Committee of Ministers. *Recommendation CM/Rec(2017)5 on standards for e-voting*. 2017. URL: https://search.coe.int/cm/#%7B%22CoEIdentifier%22:%5B%2209000016805dbef8%22%5D%7D.

[Ele26] ElectionGuard. *ElectionGuard: open-source toolkit for verifiable elections*. ElectionGuard. 2026. URL: https://electionguard.vote.

[Eli25] Eligo Social. *Standard per il voto elettronico: il Consiglio d'Europa*. 2025. URL: https://www.eligo.social/standard-per-il-voto-elettronico-consiglio-europa/.

[Eme25] EmergentMind. *End-to-End Verifiable E-Voting*. 2025. URL: https://www.emergentmind.com/topics/end-to-end-verifiable-e-voting.

[ERR23] ERR News. *Online voting: How Estonia counts, and secures, its electronic votes*. ERR News. 2023. URL: https://news.err.ee/1608906230/online-voting-how-estonia-counts-and-secures-its-electronic-votes.

[Eur22] Euronews. *Brasile, sfida elettorale Bolsonaro-Lula: sigilli anti-brogli per il voto elettronico*. Euronews / AFP. 2022. URL: https://it.euronews.com/2022/09/22/brasile-sfida-elettorale-bolsonaro-lula-sigilli-anti-brogli-per-il-voto-elettronico.

[Fon26] Fondazione Bruno Kessler – ALEPH . *E-voting: progetto di voto elettronico end-to-end verificabile*. ALEPH , Fondazione Bruno Kessler. 2026. URL: https://aleph.fbk.eu/projects/e-voting/.

[Fre26] Free & Fair. *ElectionGuard SDK: End-to-End verifiable voting*. Free & Fair. 2026. URL: https://freeandfair.us/electionguard/.

[Han26] HandWiki contributors. *Commitment scheme*. HandWiki. 2026. URL: https://handwiki.org/wiki/Commitment_scheme.

[Hel11] Helios Voting Project. *Helios v1 and v2 Verification Specifications*. 2011. URL: https://sites.google.com/site/heliosvoting/verification-specs/helios-v1-and-v2-verification-specs.

[Hel15] Helios Server Documentation. *Helios Cryptography*. 2015. URL: https://wrmack.github.io/helios-server-notes/sec_helios/.

[Hel26] Helios Voting. *Helios Voting FAQ*. 2026. URL: https://vote.heliosvoting.org/faq.

[IBM25a] IBM. *Cos'è la crittografia asimmetrica?* IBM. 2025. URL: https://www.ibm.com/it-it/think/topics/asymmetric-encryption.

[IBM25b] IBM. *Cos'è la crittografia omomorfica?* IBM. 2025. URL: https://www.ibm.com/it-it/think/topics/homomorphic-encryption.

[IBM26] IBM. *Cos'è la crittografia end-to-end*. IBM. 2026. URL: https://www.ibm.com/it-it/think/topics/end-to-end-encryption.

[Il 25] Il Giornale d'Italia. *Brasile, il partito di Bolsonaro chiede riconteggio schede elettroniche: Tribunale respinge ricorso e multa di 4,2 milioni di euro per "malafede"*. Il Giornale d'Italia. 2025. URL: https://www.ilgiornaleditalia.it/news/esteri/429245/brasile-partito-bolsonaro-chiede-riconteggio-schede-elettroniche--tribunale-multa-4-milioni-euro-malafede.html.

[Ind14] Independent E-Voting Experts. *Executive Summary: Independent Report on E-voting in Estonia – Findings Summary*. Estonia E-Voting Report. 2014. URL: https://estoniaevoting.org/findings/summary/.

[Int10] International Association for Cryptologic Research. *Helios for Cryptographers*. 2010. URL: https://www.iacr.org/elections/2010/HeliosForCryptographers.html.

[Int26] International Association for Cryptologic Research. *Requirements for eVoting Systems*. 2026. URL: https://www.iacr.org/elections/eVoting/requirements.html.

[KHC22a] Yun-Xing Kho, Swee-Huay Heng e Ji-Jian Chin. «A Review of Cryptographic Electronic Voting». In: *Symmetry* 14.5 (2022), p. 858. DOI: 10.3390/sym14050858. URL: https://www.mdpi.com/2073-8994/14/5/858.

[KHC22b] Yun-Xing Kho, Swee-Huay Heng e Ji-Jian Chin. *A Review of Cryptographic Electronic Voting*. Symmetry, MDPI. 2022. URL: https://www.mdpi.com/2073-8994/14/5/858.

[KNO23] KNOBS. *Zero-Knowledge-Proof (ZKP): cosa sono e perché sono così importanti*. KNOBS. 2023. URL: https://knobs.it/zero-knowledge-proof-zkp-cosa-sono-e-perche-sono-cosi-importanti/.

[Lak20] Josh Lake. *Can cryptography be used to secure electronic voting systems?* Comparitech. 2020. URL: https://www.comparitech.com/blog/information-security/cryptography-secure-electronic-voting-systems/.

[Lar+21] Antonio M. Larriba et al. *Distributed Trust, a Blockchain Election Scheme*. Informatica, Vilnius University Institute of Data Science e Digital Technologies. 2021. DOI: https://doi.org/10.15388/20-INFOR440. URL: https://informatica.vu.lt/journal/INFORMATICA/article/1213.

[MBC26] Emmanouil Magkos, Mike Burmester e Vassilis Chrissikopoulos. *Receipt-freeness in Large-scale Elections*. 2026. URL: https://users.ionio.gr/~emagos/I3E_receipt_freeness.pdf.

[McA25] McAfee Blog. *Hack the Vote: Pros and Cons of Electronic Voting*. Accessed: 02-02-2026. 2025. URL: https://www.mcafee.com/blogs/internet-security/hack-the-vote-pros-and-cons-of-electronic-voting/.

[Min25a] Andrea Minini. *Il sistema crittografico di Elgamal*. AndreaMinini.org. 2025. URL: https://www.andreaminini.org/crittografia/il-sistema-crittografico-di-elgamal.

[Min25b] Andrea Minini. *Il sistema RSA di crittografia spiegato in modo semplice*. AndreaMinini.org. 2025. URL: https://www.andreaminini.org/crittografia/sistema-rsa.

[Nat22] National Institute of Standards and Technology (NIST). *Improving the Usability and Accessibility of Voting Systems and Products*. 2022. URL: https://www.nist.gov/publications/improving-usability-and-accessibility-voting-systems-and-products.

[Nor24] NordVPN. *Crittografia asimmetrica: come funziona ed esempi*. NordVPN. 2024. URL: https://nordvpn.com/it/blog/crittografia-asimmetrica/.

[OSC13] OSCE Office for Democratic Institutions and Human Rights. *Handbook for the Observation of New Voting Technologies*. 2013. URL: https://odihr.osce.org/odihr/elections/new_voting_technologies.

[OSC24] OSCE Office for Democratic Institutions and Human Rights. *Handbook for the Observation of Information and Communication Technologies (ICT) in Elections*. 2024. URL: https://odihr.osce.org/odihr/elections/558318.

[OSC26] OSCE Office for Democratic Institutions and Human Rights. *Elections – OSCE/ODIHR*. 2026. URL: https://odihr.osce.org/odihr/elections.

[Par+21] Sunoo Park et al. *Going from bad to worse: from Internet voting to blockchain voting*. Journal of Cybersecurity, Oxford University Press. 2021. DOI: 10.1093/cybsec/tyaa025. URL: https://academic.oup.com/cybersecurity/article/7/1/tyaa025/6137886.

[Pia26a] Piattaforma d'informazione dei Cantoni sul voto elettronico. *Significato dei valori hash*. evoting-info.ch. 2026. URL: https://www.evoting-info.ch/it/sicurezza/significato-dei-valori-hash.

[Pia26b] Piattaforma d'informazione dei Cantoni sul voto elettronico. *Elementi di sicurezza in sintesi*. evoting-info.ch. 2026. URL: https://www.evoting-info.ch/it/sicurezza/elementi-di-sicurezza-in-sintesi.

[Pia26c] Piattaforma d'informazione dei Cantoni sul voto elettronico. *Passo per passo: scrutinio nel voto elettronico*. evoting-info.ch. 2026. URL: https://www.evoting-info.ch/it/come-funziona/passo-per-passo?step=scrutinio.

[Red22] RedshiftZero. *Commitment Schemes 101*. RedshiftZero. 2022. URL: https://redshiftzero.com/post/commitments/.

[SEC26] SECUSO Research Group, Karlsruhe Institute of Technology. *Human Factors in Electronic Voting*. 2026. URL: https://secuso.aifb.kit.edu/english/412.php.

[Seq21] Sequent Tech. *Homomorphic vs Mixnet Based E-Voting*. 2021. URL: https://sequentech.io/blog/homomorphic-vs-mixnet-based-e-voting/.

[Sta26] State Electoral Office of Estonia. *Introduction to i-voting*. Valimised.ee. 2026. URL: https://www.valimised.ee/en/internet-voting/more-about-i-voting/introduction-i-voting.

[Swi26] Swiss Post Digital. *E-voting solutions*. Swiss Post Digital. 2026. URL: https://swisspost-digital.ch/en/solutions/e-voting.

[Uni26] Unione Europea. *Accessibilità nelle elezioni*. 2026. URL: https://elections.europa.eu/it/accessibility/.

[Ver26] Verificatum. *Verificatum Mix-Net*. Verificatum. 2026. URL: https://www.verificatum.org/html/product_vmn.html.

[Wik] Wikipedia contributors. *Prêt à Voter*. Wikipedia. URL: https://en.wikipedia.org/wiki/Pr%C3%AAt_%C3%A0_Voter.

[Wik25] Wikipedia contributors. *Scantegrity*. 2025. URL: https://en.wikipedia.org/wiki/Scantegrity.

[Wik26a] Wikipedia contributors. *Blind signature*. Wikipedia. 2026. URL: https://it.wikipedia.org/wiki/Blind_signature.

[Wik26b] Wikipedia contributors. *Commitment scheme*. Wikipedia. 2026. URL: https://en.wikipedia.org/wiki/Commitment_scheme.

[Wik26c] Wikipedia contributors. *Electronic voting in Brazil*. Wikipedia. 2026. URL: https://en.wikipedia.org/wiki/Electronic_voting_in_Brazil.

[Wik26d] Wikipedia contributors. *End-to-end auditable voting*. Wikipedia. 2026. URL: https://en.wikipedia.org/wiki/End-to-end_auditable_voting.

[Wik26e] Wikipedia contributors. *Firma digitale*. Wikipedia. 2026. URL: https://it.wikipedia.org/wiki/Firma_digitale.

[Wik26f] Wikipedia contributors. *Helios Voting*. Wikipedia. 2026. URL: https://en.wikipedia.org/wiki/Helios_Voting.

[Wik26g] Wikipedia contributors. *Homomorphic encryption*. Wikipedia. 2026. URL: https://en.wikipedia.org/wiki/Homomorphic_encryption.

[Wik26h] Wikipedia contributors. *Homomorphic encryption*. Wikipedia. 2026. URL: https://en.wikipedia.org/wiki/Homomorphic_encryption.

[Wik26i] Wikipedia contributors. *Mix network*. Wikipedia. 2026. URL: https://en.wikipedia.org/wiki/Mix_network.

[Wik26j] Wikipedia contributors. *Punchscan*. 2026. URL: https://en.wikipedia.org/wiki/Punchscan.

[Wik26k] Wikipedia contributors. *Testes Públicos de Segurança do Sistema Eletrônico de Votação*. Wikipedia. 2026. URL: https://pt.wikipedia.org/wiki/Testes_P%C3%BAblicos_de_Seguran%C3%A7a_do_Sistema_Eletr%C3%B4nico_de_Vota%C3%A7%C3%A3o.

[Wir19] Wired Italia. *Il voto sulla blockchain in Russia è stato violato in 20 minuti*. 2019. URL: https://www.wired.it/attualita/politica/2019/08/21/russia-voto-blockchain/.

[Yi19] Haibo Yi. *Securing e-voting based on blockchain in P2P network*. EURASIP Journal on Wireless Communications e Networking. 2019. URL: https://doi.org/10.1186/s13638-019-1473-6.