# Review Report: On the Estonian Internet Voting System, IVXV, SoK and Suggestions for E-Vote-Id 2025 Track-3

## 1. Executive Summary

This report provides a comprehensive review of the preprint paper titled "On the Estonian Internet Voting System, IVXV, SoK and Suggestions." The paper offers a detailed Systemization of Knowledge (SoK) of the Estonian IVXV system, analyzing its historical evolution, current state, identified vulnerabilities, and recent enhancements. It also proposes several security improvements and addresses the critical, approaching challenge of quantum computing.

The paper's methodology, which involves a deep dive into the practical experiences and developments of a leading internet voting system, aligns exceptionally well with the objectives of E-Vote-Id 2025 Track-3. This track specifically calls for reports on "developments in the area of applied electronic voting" and "experiences with electronic voting or the preparation thereof," including discussions on legal, political, and social issues. The paper's granular analysis of real-world incidents, public complaints, system fixes, and the fluctuating public trust in IVXV directly addresses these requirements. Its potential to contribute significantly to the conference's discussions on real-world e-voting deployments and their inherent challenges is substantial.

The paper is well-researched, evidence-based, and offers concrete, technically sound solutions for critical issues. Its forward-looking perspective on post-quantum cryptography further enhances its relevance. This report concludes with a strong recommendation for the paper's acceptance, recognizing its valuable contribution to the understanding of complex socio-technical aspects of internet voting systems.

## 2. Introduction to the Paper and its Context

### 2.1. The Estonian IVXV System: A Pioneer in E-Voting

The paper frames the Estonian i-voting experience as "probably the richest to analyze," emphasizing Estonia's pioneering role in digital governance. Since 2001, Estonia has progressively digitized its government and private sectors, culminating in the introduction of online internet voting (i-voting) in 2005.[1] This long-standing commitment to digital public services positions Estonia's i-voting system as one of the earliest and most advanced globally.[1]

The primary objective of the paper is to present a Systemization of Knowledge (SoK) of the Estonian IVXV i-voting system. This SoK aims to provide a comprehensive overview of the system's design and structure, as well as to propose additional security enhancements. The analysis extends to applications implemented by election observers in the 2023 and 2024 elections, which the author notes have not been extensively discussed in academia previously. Furthermore, the paper examines recent fixes and improvements introduced in the June 2024 version of IVXV, connecting these changes to their academic origins. A significant forward-looking aspect of the paper is its discussion of the current system status, proposed solutions for remaining vulnerabilities, and the inevitable question of the approaching quantum threat.[1]

### 2.2. Relevance to E-Vote-Id 2025 Track-3: Election and Practical Experiences

The E-Vote-Id conference serves as a crucial forum for interdisciplinary and open discussions on all facets of electronic voting, encompassing polling stations, kiosks, ballot scanners, and internet voting.[2] Specifically, Track 3 of the conference is dedicated to reviewing "developments in the area of applied electronic voting" and reporting on "experiences with electronic voting or the preparation thereof." This includes a broad range of topics such as development and implementation reports, case law, court decisions, legislative steps, public and political debates, and election outcomes.[2] Papers submitted to this track are expected to provide an "accurate,

complete, and, where applicable, evidence-based account of the technology or system used".[2]

The paper's comprehensive SoK approach, its detailed account of the Estonian i-voting experience, and its analysis of recent developments and practical issues align exceptionally well with the stated focus of Track 3. The paper's granular detail on specific incidents, such as the Python code incident and issues with the key creation desktop, alongside its examination of real-world complaints and their resolutions, directly contributes to the understanding of practical challenges in e-voting. Furthermore, its discussion of fluctuating public trust and the underlying public and political debates surrounding internet voting in Estonia are precisely the "practical experiences" and "public and political debates" that Track 3 aims to highlight. This strong alignment positions the paper as highly suitable for this specific track, enhancing its potential for acceptance beyond its technical merits alone. The paper offers a valuable, evidence-based account of a prominent e-voting system, making it an ideal contribution to the conference's emphasis on real-world application and experience.

## 3. Analysis of IVXV System Evolution and Identified Vulnerabilities

### 3.1. Historical Context and Foundational Issues

Estonia's journey into digital governance is extensive, with digital transition beginning even before 2001. This included the introduction of e-ID cards in 2002 and the pioneering launch of i-voting in 2005.[1] Despite this early adoption and technological lead, the paper highlights a persistent "notable division within the society between those who fully trust and those who fully distrust internet voting".[1] This societal skepticism is not merely an abstract sentiment but is visibly reflected in the i-voting statistics. The ratio of i-votes, for instance, reached a peak of 51% in the 2023 local Parliament elections but subsequently declined to 41.7% in the 2024 European Parliament elections.[1] This fluctuation demonstrates that technological sophistication alone does not guarantee universal public acceptance or sustained trust; underlying

concerns, whether technical or social, can significantly impact adoption rates.

A significant foundational problem that emerged in May 2018 involved duplicate RSA keys in Estonian e-ID cards. This critical security flaw was traced back to Gemalto, the manufacturing company, which had generated the RSA keys outside the chip, violating agreed-upon security protocols.[1] This incident, which became a global crisis for the company, underscored the profound importance of secure key generation and the lasting impact of foundational cryptographic weaknesses on public infrastructure. In response, Estonia shifted its core cryptographic components, moving towards threshold cryptography and homomorphic encryption. The IVXV system now employs 384-bit Elliptic Curve Cryptography (ECC) with El-Gamal Encryption, although it is important to note that the list of authorized votes continues to be signed using a 2048-bit RSA key.[1]

The evolution of the Estonian i-voting system into its current IVXV form has been marked by several key milestones. Initially, the system utilized a double envelope protocol since 2005. A pivotal development occurred in 2013 with the introduction of voter verification capabilities, a feature prompted by a student's demonstration of proof-of-concept ballot-manipulating software in 2011.[1] In 2017, Cybernetica partnered with Smartmatic to develop the new IVXV design, which incorporated a vote-registration service to prevent vote dropping, a shuffling re-encryption mix-net to ensure vote privacy, and Schnorr-based non-interactive zero-knowledge proofs (NIZKPs) to cryptographically verify the integrity of the mix-net output.[1] These advancements aimed to bolster both the verifiability and privacy aspects of the voting process. The persistent societal division regarding i-voting trust is not merely a sociological phenomenon but is exacerbated by and directly reflects these actual technical incidents. The 2018 RSA key vulnerability and the earlier ballot manipulation demonstration are concrete examples of technical flaws that directly contribute to public distrust and skepticism, as evidenced by the fluctuating i-vote statistics. Even when technical fixes are implemented, the historical baggage of such incidents can persist in public consciousness, impacting adoption rates and overall confidence in the system.

### 3.2. Technical Incidents and Community Concerns

The paper highlights several technical incidents and community concerns that have impacted the perception and security of the IVXV system. A notable incident in the

2023 elections involved a computer scientist observer who successfully voted using their own Python code.[1] This event raised a significant alarm, as it demonstrated that the voting application (VA), which voters download to cast their ballots, is "not authenticated by the system." The OSCE report also recognized this as a potential cybersecurity risk.[1] This points to a critical "last mile" vulnerability, where a malicious client-side application could potentially compromise the integrity of the voting process, even if the backend infrastructure is robust.

Another area of concern arose from complaints regarding the desktop used for key creation during the setup phase of elections. It was alleged that this critical machine was not completely isolated and had extra software installed on it.[1] An observer documented this by taking a photograph during a disk inspection, subsequently pursuing the matter through the supreme court. While the court concluded that this could not have affected the voting results, IVXV representatives later acknowledged the risk and stated that it had been addressed.[1] This incident underscores the importance of stringent operational security measures, particularly during sensitive phases like key generation, to prevent potential insider threats or unintentional vulnerabilities.

A recurring observation made by the authors is that many complaints, even those with clear technical merit, are frequently rejected without objective investigation, often citing strict submission deadlines.[1] The OSCE 2025 report has also commented on this issue, recommending that legislators consider the specific complexities of internet voting when setting appropriate deadlines.[1] This practice of rejecting complaints without thorough, transparent investigation can erode public trust and contribute to ongoing skepticism.

The decryption of invalid votes has also been a source of controversy. Following the 2024 European Parliament elections, a complaint regarding this issue was rejected, partly on the grounds that the complainant was an observer, not an authorized auditor.[1] Although IVXV remediated its code to generate proofs of correct decryption for invalid votes before June 2024, the file containing this decryption remains accessible only to auditors.[1] The paper critically analyzes the justifications for this restriction, citing Kraavi's master thesis for a more scientific perspective on the potential for information leakage or encoding attacks. The authors also note a "suspiciously" constant number of invalid votes (denoted as 'I') in the last three local elections since 2021, which they find raises doubts about the process.[1]

Beyond these specific incidents, the paper mentions other opposition activities, such as an observer developing a "shadow e-voting site" or "virtual threshold survey" to

encourage citizens to re-vote as a form of check.[1] Furthermore, a report from the Cyber Security Committee of the Academy of Sciences in June 2024 identified six threats with a risk class higher than "small," indicating that problems persist within the system.[1]

The recurring pattern of "silent fixes" [1], IVXV's reported lack of communication with researchers [1], and their described "offensive than scientific" tone [1] collectively point to a systemic issue of transparency deficit. This lack of openness directly contributes to the persistence of opposition complaints and exacerbates the "societal division" [1] regarding trust in i-voting. When authorities do not openly acknowledge or discuss vulnerabilities, even after fixing them, it creates an environment where every technical incident, no matter how minor, can be magnified by the opposition and further erode public confidence. The low QR verification ratio, reported at 5.5-9.9% [1], can be seen as a symptom of this broader trust issue, as voters may not engage with verification mechanisms if they already distrust the system's underlying processes or the communication surrounding them.

### 3.3. Cryptographic Attacks and System Weaknesses

The paper provides a detailed examination of specific cryptographic vulnerabilities that have been identified and, in some cases, addressed within the IVXV system.

#### The El-Gamal C1/C2 Manipulation Exploit (Fixed 2023)

An exploit discovered in 2022 by and subsequently fixed by IVXV in 2023, revealed a critical flaw in the El-Gamal encryption scheme's implementation. In the older design, the verification application (VA) only received the C2 component of the encrypted vote from the vote collector. This allowed a malicious voting application to manipulate the encrypted ciphertext by sending different C1 values for the same C2. Without verifying the C1 value, the verification application would fail to detect fraud if the voting application sent an incorrect random number (r') to the vote collector, such that y^r * v = y^r' * v' (where y is the public key, v is the vote, and r is the random number), thereby deceiving the vote collector into recording a manipulated vote.[1]

The fix, implemented on February 23, 2023, just before the March 2023 elections, involved the vote collector sending the entire encrypted pair (C1, C2) to the verification application. The verification application was updated to also verify that C1 = g^r (where g is the generator for El-Gamal encryption).[1] While this specific cryptographic flaw was patched, the paper cautions that the risk persists for non-verifying voters who might be using a malicious voting application or operating within a compromised communication network.[1] The authors express concern that such a "straightforward vulnerability wasn't noticed earlier" [1], leading to a broader critique of IVXV's overall quality.

**Pereira Attack (2022) and its Generalization**

Olivier Pereira's work in 2022 uncovered an attack where a malicious voting application could simulate a system crash to trick a voter into casting their vote multiple times.[1] This deceptive maneuver allows the malicious application to capture the voter's digital signature twice, enabling it to construct and sign a new encrypted vote in the background. Simultaneously, the application would display the QR code corresponding to the voter's original, intended choice, while the system ultimately counts the newly generated, potentially manipulated vote.[1]

A formal verification study by Baloglu et al. in 2024 not only rediscovered this specific attack but also identified a more generalized timing attack. This generalized attack, akin to Pereira's "Ghost Click" attack, involves an adversary storing a fake ballot and submitting it as late as possible to ensure it is counted.[1]

**End-to-End Verifiability (EEV) Limitations**

Recent formal verification analyses, such as that conducted by Baloglu et al. on earlier IVXV versions, have indicated limitations in the system's End-to-End Verifiability (EEV). Their findings suggest that EEV+ (an enhanced form of EEV) fails if an adversary gains control over more than a certain number of voters' credentials, or if two of the core system components—the Vote Collector (VC), the Registration Service (RS), or the timestamping service (TMS)—collude.[1] This implies that while IVXV aims for comprehensive EEV, its practical implementation still relies on certain trust

assumptions that could be exploited under specific adversarial models.

A consistent and critical vulnerability highlighted throughout the paper is the client-side voting application (VA). The Python code incident, the C1/C2 manipulation exploit, and the Pereira attack all originate from or are exacerbated by the VA.[1] The core issue is that the VA's code is "unrevealed" (not open source) and "not authenticated by the system".[1] This creates a dangerous "last mile" where even a cryptographically sound backend can be undermined by a malicious client. This risk is further amplified by the low QR verification ratio, reported at 5.5-9.9% [1], indicating that the vast majority of voters do not perform the optional verification steps that could detect such client-side compromises. This suggests a fundamental design flaw in assuming a trustworthy client environment, which in practice, represents a significant attack surface.

**Table 1: Summary of IVXV Vulnerabilities and Corresponding Fixes/Proposed Solutions**

| Vulnerability/Issue | Nature of Threat/Impact | IVXV's Response/Fix | Paper's Assessment of Fix | Proposed Solution (by paper/others) |
|---|---|---|---|---|
| RSA Key Duplication (e-ID) | Compromised key generation, potential for identity theft/forgery | Migration to ECC/El-Gamal for IVXV core, changed ID card manufacturer, remote fixes for existing cards | Addressed for core crypto, but RSA still used for vote list signing. | N/A (addressed by migration) |
| Unauthenticated Voting Application (VA) | Malicious VA can manipulate votes, enable coercion/buying, undetected by system | None (VA code unrevealed, not authenticated by system) | Persisting, high risk for non-verifying voters. | Publish VA hash/Sign VA; Verification app message; Registered VAs with authentication keys; Direct voter warning. |
| El-Gamal C1/C2 | Malicious VA | Vote collector | Partially | N/A (fix |

| | | | | |
|---|---|---|---|---|
| Manipulation | sends wrong C1, deceives vote collector | sends (C1, C2) to verification app; Verification app verifies C1=g^r | mitigated; risk remains for non-verifying voters or compromised networks. | implemented, but underlying VA issue persists) |
| Invalid Votes Access/Transparency | Observers denied access to invalid vote decryption proofs; suspicious constant count of invalid votes | Invalid votes in separate file with ZKPs for decryption | Partially mitigated; transparency issue persists due to restricted access. | Range Proofs (ZKPs) at Vote Collector to reject invalid votes earlier. |
| Key Creation Desktop Security | Extra software on key creation desktop, potential for malware/insider threat | IVXV admitted risk, stated it was "taken care of" (details not specified) | Partially mitigated (fix details unclear); points to operational security gaps. | N/A (IVXV claims fix, but details are opaque) |
| Insider Risk at Processing Stage (Ballot Processor) | Manipulation of "to be counted" vote list (e.g., adding removed multiple votes) | Integritytool.java implemented (SHA256 hashes, count-based validation) | Partially mitigated; depends on trusting VC/RS for initial input integrity. | Overall checks with e-government data (myID service); Verkle Trees for cryptographic commitment to vote counts. |
| Pereira Attack (Fake Crash-Restart) | Malicious VA captures multiple signatures, submits new vote while showing old QR | Session ID check before QR generation | Partially mitigated; original fast-sequencing attack still persists. | Session tracking number in QR code (unadopted suggestion); Force time interval between votes. |
| Quantum Threat | Shor's Algorithm can break El-Gamal encryption, "Harvest Now | Active PQC research/collaboration in Estonia (Cybernetica, Tartu Uni, EU | Unaddressed for current IVXV implementation; ongoing R&D. | PQC migration for all cryptographic components (e.g., |

| | | | | |
|---|---|---|---|---|
| | Decrypt Later" risk | initiatives) | | Lattice-based, Hash-based signatures). |

## 4. IVXV's Responses and Implemented Enhancements

### 4.1. Addressing Past Exploits

The paper details how a significant exploit, introduced in 2022 by , which allowed for the manipulation of encrypted votes through the El-Gamal C1/C2 components, was addressed and fixed by IVXV in 2023.[1] The resolution involved modifying the system so that the vote collector sends the entire encrypted pair (C1, C2) to the verification application. This application was then updated to verify that C1 equals

g^r (where g is the generator and r is the random number), thereby preventing the malicious manipulation observed previously.[1] This fix was deployed on February 23, 2023, just prior to the March 2023 elections.[1]

Despite the implementation of this fix, the authors voice concern that such a "straightforward vulnerability wasn't noticed earlier" [1], leading to a broader critique of the overall quality of the IVXV system's security posture. More critically, they emphasize that the risk associated with this type of manipulation "remains for nonverifying voters with either a malicious voting application or a malicious communication network".[1] This highlights that while the specific cryptographic flaw was patched, the underlying vulnerability related to client-side trust and the low rate of voter verification continues to pose a risk. The belated discovery of a "straightforward" cryptographic vulnerability and its subsequent fix, while necessary, points to a reactive rather than proactive security development lifecycle within IVXV. This consistent pattern suggests that IVXV's security enhancements are often targeted patches addressing specific reported exploits, rather than a fundamental re-evaluation of its trust assumptions or a comprehensive strategy to mitigate broader classes of attacks, especially those involving the client-side voting application or voter

behavior.

### 4.2. Handling Invalid Votes and Integrity Checks

IVXV has made enhancements to its handling of invalid votes. These votes are now segregated into a separate file, and Zero-Knowledge Proofs (ZKPs) are generated to cryptographically assure their correct decryption.[1] However, a significant point of contention remains: election observers are explicitly "not allowed to access this file or verify those proofs," leading to ongoing debate and complaints regarding transparency.[1] The paper critically analyzes the official justifications for this restriction, such as technical infeasibility or the potential for encoding attacks, by referencing Kraavi's master thesis for a more scientific rationale.[1] The authors also note a "suspiciously" constant number of invalid votes (denoted as 'I') in the last three local elections since 2021, which they suggest raises questions about the process.[1]

In terms of broader integrity, a partial safeguard against insider risks during the ballot processing stage has been integrated into IVXV's audit application through the Integritytool.java file.[1] The academic details of this solution were only published in in December 2024. This implementation applies checks to the Ballot Processor data, utilizing SHA256 hashes and count-based validation (e.g., verifying

Count (original votes file) - Count (anonymous valid votes) = Count (multiple votes) + Count (replaced by paper) + Count (invalid votes)) to detect manipulations such as the re-introduction of removed older multiple votes.[1]

A crucial limitation of these integrity checks is highlighted in the paper: the "integrity of those cryptographic checks (like the Count (original votes file)) depends on trusting the vote collector and the registration application to not collude".[1] This means that while the implemented solution helps mitigate collusion

*within* the Ballot Processor, it does not address the significant insider risk posed by potential collusion between the Vote Collector (VC) and the Registration Service (RS), leaving a critical vulnerability unaddressed.[1] The decision to restrict access to invalid vote decryption proofs to a narrow "circle of trust" (auditors only) and the reliance on trusting the Vote Collector and Registration Service for initial vote counts fundamentally undermines the principle of universal verifiability. While valid privacy concerns for invalid votes exist, the "suspiciously constant number" of invalid votes,

combined with the lack of public verifiability for their decryption, creates a significant transparency gap. This approach prioritizes a limited trust model over open, cryptographic proof, potentially fueling public distrust and making it harder to definitively refute claims of manipulation, which directly contradicts the goals of a transparent election system.

### 4.3. Session Management and Time Checks

In response to the Pereira attack, where a malicious voting application could trick a voter into re-voting by faking a system crash, IVXV deployed a solution on May 30, 2024.[1] The updated code now checks if the session-ID remains the same before generating the verifying QR code. The documentation for this change indicates its purpose is to "prevent reusing session ID until it is deleted from a database or expired".[1]

However, the paper, supported by formal verification from Baloglu et al. , argues that this solution "cannot handle the original attack in , since it depends on the fast sequencing of the fake crash-restart scenario".[1] This allows a malicious voting application to reuse an unexpired session ID with a reasonable time difference, effectively bypassing the current checks.[1] An independent analysis by an AI companion (Grok) also confirmed the persistence of this threat.[1] This illustrates that while IVXV implemented a technical control, the original attack vector, which exploits subtle timing and behavioral aspects, remains viable.

Previous suggestions to mitigate this vulnerability, such as advising voters to double-check transactions with the myID service, verifying only the last vote, or adding a flag to the QR code indicating if it is the last vote, do not appear to have been adopted by IVXV.[1] The partial nature of IVXV's fix for the Pereira attack exemplifies the ongoing "cat and mouse" game in cybersecurity. While IVXV implemented a technical control (session ID check), the paper, supported by formal verification and AI analysis, demonstrates that the original attack vector (fast sequencing of fake crash-restart) remains viable. This highlights that security solutions must not only address known exploits but also anticipate adversarial ingenuity. A failure to fully close an attack vector, even after a fix, can lead to a false sense of security and leave the system vulnerable to persistent threats that exploit subtle timing or behavioral aspects.

## 5. Proposed Solutions and Future Directions

### 5.1. Authenticating the Voting Application

The voting application (VA) represents a significant vulnerability within the IVXV system, primarily because its code is not open source and the application itself is not authenticated by the system.[1] This lack of transparency and authentication creates a critical attack surface, allowing for the potential deployment of malicious VAs, particularly targeting the vast majority of voters (90-95%) who do not perform the optional vote verification steps.[1] The paper warns of severe implications, including "DarkDAOs" and "massive vote buying/coercion," where an adversary could control voters through compromised VAs, forcing them to cast specific votes without their knowledge or consent.[1]

To address this critical "last mile" vulnerability, the paper proposes several safeguards:

- **Publishing File Digest:** A straightforward and moderate safeguard involves publishing the SHA256 hash of the official VA code. Voters could then be encouraged to run a check on their downloaded application before use, similar to how the Electrum Bitcoin wallet verifies its binaries.[1] This method is considered more robust than relying solely on the operating system's verification of a developer key signature.[1]
- **Verification Application Message:** For voters who do utilize the QR code verification process, the verification application could display an additional message. This message would inform the voter whether they cast their vote using the official voting application or a "different" (unofficial) one.[1] This approach aligns with IVXV's stated philosophy of allowing voters the freedom to use their own trusted applications, while still providing a crucial security alert.[1]
- **Registered Applications with Authentication Keys:** A more robust and non-optional solution involves assigning a unique signature and authentication key pair to the official voting application. The election authority would then only permit the use of pre-registered VAs whose public keys are stored on the voting

server. This mechanism would allow the election authority to scan private voting applications for malicious or vote-buying code before granting them usage rights.[1]

- **Direct Voter Warning:** To ensure non-verifying voters are informed if their vote was rejected due to a malicious VA, the vote collector could deduce the voter's IP address from the initial contact with the VA. A direct warning message, such as a pop-up on the voter's screen stating "Be careful, this is not the official voting application," could then be sent.[1] This leverages IVXV's existing capability to determine IP addresses, used for calculating the ratio of abroad voters.[1]

All these proposed solutions can be made post-quantum secure by integrating hash-based digital signatures, such as the Stateless Hash (SLH)-DSA. Although SLH-DSA has a relatively large size (7k Byte), this would only be transmitted once during the initial download and would likely not be noticeable by users.[1] The strong emphasis on authenticating the voting application is a direct, necessary response to the "last mile" vulnerability. The discussion of "DarkDAOs" and "massive vote buying/coercion" elevates the unauthenticated VA from a mere technical flaw to a severe threat to democratic integrity, demonstrating how a seemingly small technical vulnerability can have profound societal implications. The success of these solutions also inherently relies on user engagement, such as checking hashes or reading warnings, underscoring that e-voting security is not purely a technical problem but a socio-technical one requiring active voter participation and awareness.

### 5.2. Enhancing Ballot Integrity and Insider Risk Mitigation

The paper identifies a critical vulnerability in IVXV: the integrity of the initial input file, which originates from the Vote Collector (VC) and Registration Service (RS), is not cryptographically proven, leaving it susceptible to insider manipulation.[1]

To address this, the paper suggests several approaches:

- **Range Proofs for Invalid Votes:** To eliminate complaints and risks associated with invalid votes, the paper proposes preventing them from reaching the Ballot Processor entirely. This would involve the Vote Collector application performing a Zero Knowledge Proof (ZKP) check, specifically a Range Proof, to verify the validity of the vote it receives from the voting application without revealing the vote's content. This would allow invalid votes to be rejected earlier in the process.[1]

The paper favors Range Proofs based on Bullet Proofs and Pederson Commitments, citing their compatibility with El-Gamal encryption and faster prover times compared to general-purpose SNARKs.[1]

- **Overall Checks with E-Government Data:** As an alternative or complement to purely cryptographic proofs for initial vote counts, the paper suggests leveraging Estonia's robust existing e-government infrastructure. This approach involves comparing the total number of transactions to IVXV services with other data records available in the Estonian Information System, such as the myID service.[1] This could include verifying the total count of ballots and potentially performing Risk Limiting Audits (RLAs). In RLAs, a sample of random votes from IVXV could be manually checked against corresponding e-government transaction records, effectively using the e-government data as a "paper ballot" equivalent for verification.[1]
- **Proposed Verkle Tree for Cryptographic Commitment:** The paper suggests a more robust protection against insider risks by proposing the cryptographic commitment to each vote spontaneously using Authenticated Data Structures (ADSs), specifically Verkle Trees.[1] Verkle Trees are a type of vector data structure that authenticate their elements based on KZG polynomial commitments, and crucially, they can cryptographically prove the *number* of elements stored within them.[1]
    - This mechanism would aggregate vote hashes, preventing ballot stuffing and dropping even if the Vote Collector and Registration Service colluded.[1]
    - Verkle Trees offer constant order complexity SNARKs. While they require a trusted setup procedure to generate a common reference string (crs), this setup is universal (not circuit-specific like Groth16) and aligns with IVXV's existing setup and key generation phase.[1] This arrangement also facilitates the use of Risk Limiting Audits (RLAs) to verify the details of a selected sample of ballots.[1]
    - The paper argues for the superiority of Verkle Trees over traditional Merkle Trees, which do not verify total and subtotal numbers, a critical requirement for ballot integrity.[1] It also contrasts Verkle Trees with STARKs, noting that while STARKs offer post-quantum security and do not require a trusted setup, these advantages are less relevant if the underlying encryption (El-Gamal) is not post-quantum secure.[1] If quantum computing becomes feasible, an adversary could discover private keys and produce correct values that would pass verifier checks, making STARKs only a better solution if they are compatible with a post-quantum update of the underlying encryption.[1]
    - A significant additional benefit of Verkle Trees is the ability to keep the generated trees as permanent proof, even after the original election data is

destroyed (e.g., after a month), by allowing the verifier to check the generated proof instead of the original data.[1]

The paper's proposals for enhancing ballot integrity, particularly the Verkle Tree concept, represent a fundamental paradigm shift from relying on human trust (e.g., trusting VC/RS not to collude) to establishing cryptographic guarantees for the integrity and count of votes. The "suspiciously constant number of invalid votes" and the inherent "insider risk" are symptoms of a system where too much trust is placed in specific entities. By advocating for Authenticated Data Structures that cryptographically prove the number of ballots, the paper pushes towards a more robust "universal verifiability" model, significantly reducing the "circle of trust" and enhancing public confidence through mathematical certainty rather than mere procedural assurances.

**Table 2: Comparison of Proposed Authenticated Data Structures for Ballot Integrity**

| Feature/Criterion | Verkle Tree | Merkle Tree | STARK |
|---|---|---|---|
| Cryptographic Proof of Element Count | Yes (via KZG polynomial commitments) | No (only integrity of elements/order) | Yes (via FRI commitments) |
| Proof Complexity | Constant order (per node or batch) | Logarithmic | Scalable (often better than SNARKs for large data) |
| Trusted Setup Required | Yes (universal setup) | No | No |
| Post-Quantum Security | No (depends on underlying crypto) | Yes (if hash function is PQ) | Yes (based on hash functions/FRI) |
| Compatibility with El-Gamal | Yes (discrete logarithm problem) | Yes (hash function agnostic) | Yes (can be applied to El-Gamal based systems) |
| Suitability for Batching/Archiving | Yes (homomorphic property, permanent proof) | Yes (for integrity checks) | Yes (for integrity checks, permanent proof) |

### 5.3. The Post-Quantum Cryptography Imperative

The paper emphasizes the "inevitable question of the approaching quantum threat" [1], underscoring its critical implications for current cryptographic systems. Shor's Algorithm, a quantum algorithm, has the theoretical capability to break cryptographic functions based on the Discrete Logarithm and Elliptic Curve problems, including the El-Gamal encryption currently used by IVXV.[1] This poses a significant "Harvest Now Decrypt Later" (HNDL) threat, where encrypted data collected today could be stored by adversaries and decrypted in the future once sufficiently powerful quantum computers become available.[1]

The paper highlights the accelerating pace of quantum computing advancements. It references Google and Microsoft's unveiling of their first quantum chips in December 2024, a competition offering 1 BTC to break a Bitcoin key using quantum computing by April 2026, and significant European financial sector investments in Post-Quantum Cryptography (PQC), with plans for $1 billion in 2025.[1] These developments underscore the growing urgency for cryptographic systems to migrate to quantum-resistant algorithms.

Main solution strategies for PQC include those based on Lattice cryptography (e.g., Kyber, ML-KEM), Hash functions (e.g., SLH-DSA), multivariate equations, and error-correcting codes.[1] NIST has already finalized three PQC standards.[1] However, security analyses of candidates like CRYSTALS-Kyber (the basis for ML-KEM) have identified potential vulnerabilities, including side-channel attacks.[1]

Estonia is actively involved in various quantum-related initiatives. These include participation in a European quantum communication infrastructure established in 2020, the NordIQuEst project in 2022, and a collaboration between Cybernetica (the company behind IVXV) and the University of Tartu since 2021 to develop post-quantum solutions.[1] Additionally, PQC is one of six challenge areas within a Cyber Security hub established in 2023 between Estonia and a major Czech ICT powerhouse.[1] The European Commission further published a coordinated PQC implementation roadmap for member countries in April 2024, recommending "hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution (QKD)".[1]

Despite these proactive efforts, IVXV faces specific PQC challenges. While

Cybernetica announced the certification of a post-quantum ID card chip in February 2025, they acknowledged that "there is more math to do" for i-voting systems.[1] The paper notes that the complexity of managing multiple layers in hybrid systems could be a disadvantage for IVXV, particularly with its reliance on mix-nets for vote shuffling. In this context, lattice-based approaches might offer advantages due to their reliance on matrix operations.[1] The detailed exposition of the quantum threat is not merely a technical discussion but a critical strategic imperative for IVXV. The "Harvest Now Decrypt Later" (HNDL) threat fundamentally shifts the timeline of security, implying that even currently secure data could be retroactively compromised. While Estonia has shown proactive efforts in PQC research, Cybernetica's admission that "there is more math to do" for i-voting and the identified complexities of hybrid systems for mix-nets reveal that the practical implementation of quantum-safe cryptography for a system as complex as IVXV is a significant, unsolved engineering and cryptographic challenge. This highlights that the transition is not just about replacing algorithms but about re-architecting core cryptographic components under new performance and security constraints, requiring substantial, long-term research and development.

### 5.4. Suggested Research Directions

The paper concludes by outlining several promising research directions that emerge from its comprehensive analysis, reflecting the multifaceted nature of e-voting security:

- **Hardware Acceleration of ZKPs:** Future research could build upon existing work, such as that in , to delve deeper into circuit-specific details and efficient hardware implementations of Zero Knowledge Proofs.[1]
- **Theoretical Cryptographic Proofs:** Further exploration of advanced mathematical proofs, drawing from theoretical works like , could enhance the foundational understanding of cryptographic protocols in e-voting.[1]
- **Comparative Analysis of ZKPs:** There is a need for in-depth comparative analysis of various zero-knowledge proofs, focusing on their implementation details and proof batching reductions specifically tailored to the 384-bit elliptic curve used in IVXV.[1]
- **Quantum Secure Solutions:** Continued research is essential for developing efficient quantum-secure solutions, conducting cryptanalysis of new Post-Quantum Cryptography (PQC) protocols, and formally verifying these protocols to ensure their correctness and security in a post-quantum era.[1]

- **AI-based Attacks:** Investigation into the role of Artificial Intelligence in developing sophisticated side-channel attacks and exploring potential new attack vectors against cryptographic components and emerging quantum devices presents a rich research area.[1]
- **Digital Identity Logs and Coercion:** A broader research avenue involves examining how general-purpose activity logs of digital identities (e.g., Estonia's myID service) could be exploited by vote buyers or coercers. This includes understanding the implications for blockchain-based e-government systems and the trade-offs between data availability for integrity checks and potential privacy compromises.[1]

The diverse range of suggested research directions underscores that the future of e-voting security is inherently interdisciplinary. It extends beyond traditional cryptography to encompass hardware acceleration, formal methods, artificial intelligence, and socio-technical considerations like the privacy implications of digital identity logs for vote buying/coercion. This indicates that comprehensive security for advanced e-voting systems requires a convergent approach, drawing expertise from computer science, mathematics, and even social and political sciences, moving beyond isolated technical fixes to address the complex interactions within the broader digital ecosystem.

## 6. Critical Assessment and Suitability for E-Vote-Id 2025 Track-3

### 6.1. Strengths of the Paper

The paper demonstrates several significant strengths that make it a valuable contribution to the field of electronic voting:

- **Comprehensive Systemization of Knowledge:** The paper provides a highly detailed and timely Systemization of Knowledge (SoK) of the Estonian IVXV system. This encompasses its historical evolution, current architectural design, and recent developments, offering a holistic view of a prominent internet voting system.[1]
- **Timely and Relevant Analysis:** Its focus on very recent incidents from the 2023

and 2024 elections, along with an analysis of corresponding fixes, ensures that the paper is highly current and directly relevant to ongoing discussions within the e-voting community.[1]

- **Practical Focus:** By thoroughly analyzing a live and widely used internet voting system, the paper offers invaluable insights into real-world challenges and practical solutions. This aligns directly with a core objective of E-Vote-Id Track-3, which emphasizes applied electronic voting and practical experiences.[1]
- **Evidence-Based Approach:** The paper rigorously supports its claims and analyses by citing a wide array of credible sources, including academic literature, official OSCE reports, supreme court decisions, and direct references to IVXV's public code repositories.[1] This robust evidence base enhances the paper's credibility and academic rigor.
- **Identification of Unnoticed Work:** A commendable aspect of the paper is its effort to highlight previously "unnoticed" academic work, such as formal verification studies of IVXV. This enriches the overall analysis and brings important, overlooked research to the forefront.[1]
- **Concrete Proposed Solutions:** Beyond merely identifying vulnerabilities, the paper proposes concrete, detailed, and technically sound solutions for critical issues, particularly concerning voting application authentication and ballot integrity. These proposals are well-reasoned and actionable.[1]
- **Forward-Looking Perspective:** The paper's robust discussion of the quantum computing threat and its implications for IVXV demonstrates a forward-looking and proactive approach to e-voting security, addressing a future challenge that will inevitably impact cryptographic systems.[1]

### 6.2. Areas for Improvement

While the paper is of high quality, a few areas could be further strengthened to enhance its impact:

- **Depth of Technical Feasibility for Proposals:** While the proposed solutions, such as the use of Verkle Trees or direct voter warnings via IP addresses, are conceptually strong, the paper could benefit from a more in-depth discussion of their practical implementation challenges. This includes considerations of performance implications at IVXV's scale, integration complexities within the existing system architecture, and potential trade-offs. For instance, the persistence of the "Ghost Click" attack, even after IVXV's fix, could lead to a

deeper discussion on the inherent trade-offs between usability and security in client-side design.

- **Nuance in Critical Stance:** The paper's critical tone regarding IVXV's transparency and communication, while largely justified by the presented evidence, could be refined to present the observations with slightly more academic nuance. For example, framing IVXV's "offensive" tone as an "observed communication style" rather than a direct accusation might maintain an even stronger objective voice, which is generally preferred in academic discourse.
- **Privacy Implications of "Overall Checks":** The proposed "Overall Checks" that leverage myID service data for ballot integrity, while beneficial for enhancing verifiability, could warrant a more explicit discussion of their privacy implications. Given the paper's own focus on privacy attacks, acknowledging and potentially suggesting mitigations for any new privacy concerns arising from linking voting records to broader digital identity transaction logs would strengthen the analysis.

### 6.3. Alignment with Track-3 Objectives

The paper is an exceptionally strong candidate for submission to E-Vote-Id 2025 Track-3. Its comprehensive "Systemization of Knowledge" of a real-world, operational e-voting system, coupled with detailed reports on "experiences" including technical incidents, fixes, public complaints, and the system's evolution, directly fulfills the track's primary objectives. It is not a purely theoretical paper but a practical review, which is precisely what Track 3 aims to publish, making it an ideal submission for this specific conference track.

The paper directly addresses the track's call for "Review developments in the area of applied electronic voting" and "Report on experiences with electronic voting or the preparation thereof".[2] It provides an "accurate, complete, and, where applicable, evidence-based account of the technology or system used".[2] Furthermore, the paper delves into "Legal, political and social issues" (e.g., societal division, court decisions, complaints, OSCE reports) and "Administrative, legal, political and social issues" [2], which are explicit themes for Track 3. The inclusion of "suggestions for further future research" [1] also aligns well with the conference's broader goal of fostering new ideas and discussions within the e-voting community.[2]

## 7. Conclusion and Recommendation

This paper provides a comprehensive and timely Systemization of Knowledge of the Estonian Internet Voting System (IVXV), offering a valuable historical, technical, and social context for its development and current status. It meticulously surveys existing academic literature and other available resources to detail reported attacks, vulnerabilities, and IVXV's responses, including recent enhancements in the June 2024 version.

The authors effectively address concerns raised by opposing parties and researchers, proposing concrete, well-reasoned solutions for critical remaining vulnerabilities. Key recommendations include authenticating the voting application to mitigate client-side risks, which the paper argues is of significant concern. This is supported by the observation that the "encrypted copy attack is of higher risk level and nonnegligible probability".[1] Additionally, the paper proposes enhancing ballot integrity against insider manipulation through methods like overall consistency checks leveraging existing e-government data and the innovative use of Authenticated Data Structures such as Verkle Trees.

Furthermore, the report highlights the critical and approaching quantum computing threat to e-voting systems and digital identities in general, providing an overview of Estonia's proactive efforts and outlining promising future research directions.

The paper's strong evidence-based approach, its focus on practical experiences, and its timely analysis of a leading e-voting system make it an excellent fit for E-Vote-Id 2025 Track-3. Its insights into the interplay of technical security, public trust, and the operational realities of a long-standing internet voting system are invaluable for the broader e-voting community.

**Recommendation:** This paper is highly recommended for acceptance to E-Vote-Id 2025 Track-3. Its contributions are significant for understanding the complexities of real-world e-voting deployments and for guiding future security enhancements. The paper's concluding advice for IVXV to engage more scientifically and objectively with external scrutiny is also well-founded, as such transparency would undoubtedly enhance public trust and recognition for their ongoing work.

**Works cited**

1. Estonia_preprint_10_7_25.pdf

2. E-Vote-ID 2023 - E-Vote-ID – The International Conference for Electronic Voting, accessed July 10, 2025, https://www.e-vote-id.org/e-vote-id-2023/
3. E-Vote-ID 2025, accessed July 10, 2025, https://e-vote-id-2025.inria.fr/
4. E-Vote-ID – The International Conference for Electronic Voting, accessed July 10, 2025, https://www.e-vote-id.org/