¡Olé! Insights from Remote Voting in the 2024 Mexican Federal Election

Voatz, Inc.
voatz.com

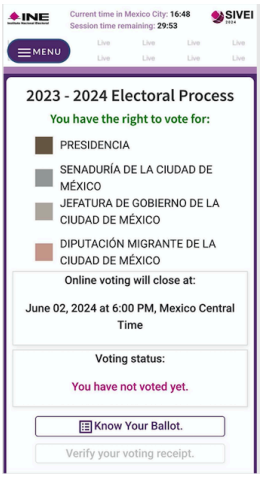
On June 2, 2024, the national and local elections were held in Mexico for the office of the President, 128 Senate seats, and for the office of the Governor in 9 of the 32 states. The majority of Mexican citizens voted in person at the polls in these historic elections wherein Mexico elected its first woman President. Also for the first time, Mexican citizens living outside the country were able to vote online or using an electronic voting kiosk at one of 23 embassies or consulates in the U.S., Canada, and Europe.

In this article, we will explore several unique elements of this election. Section 1 describes the **election administration** of their remote voting. Section 2 highlights Mexico's **voter education** program. Section 3 describes the **cybersecurity** technology used to secure remote voting and to enable the electoral authority to generate provable election results within minutes of the close of the election. That leads to important and interesting policy questions that arise in Section 4.

1. Election administration

Pre-election simulations

Prior to the election, two iterative **simulations** of remote voting were held in April 2024. Each week-long simulation served as a **logic and accuracy test** of the whole system by the national election authority. Administration tasks were live-streamed for observation by regional officials, candidates, political parties, auditors, citizens, and the media. Thousands of mock ballots were cast to ensure that the contests were displayed, marked, recorded, tallied, and reported correctly in the test environment. Mock in-person kiosk voting occurred on the last day of each simulation.



Remote voting dashboard (English)

Election period operations

Remote Voting: Registered expatriate voters who elected to vote remotely on their own device received an email with their onboarding credentials. Once voters verified their contact information and completed two-factor authentication, they were able to log in and vote from the dashboard shown above. After voting, they received a voting receipt code on screen, in a downloadable PDF, by email, and by SMS. On the voting system's dashboard, they could enter their voting receipt code to verify that their ballot was received unmodified.

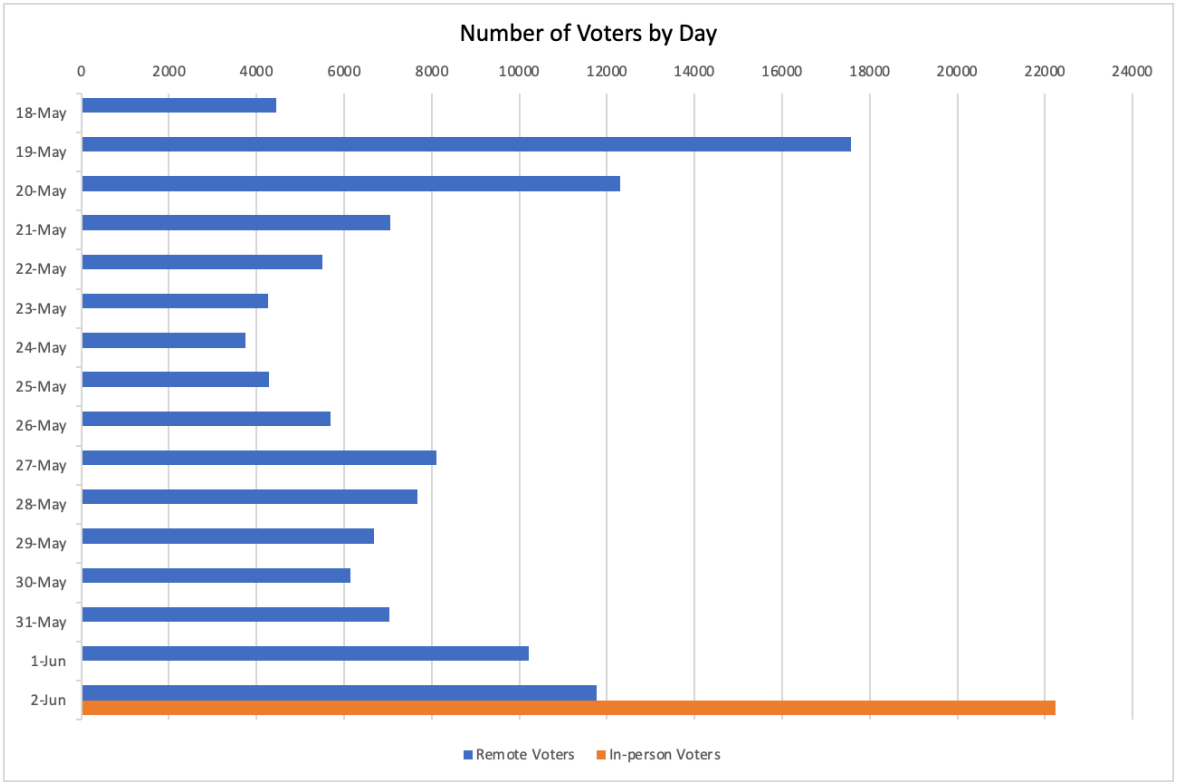
Kiosk Voting: At the embassies and consulates, voters verified their identity to official personnel to receive an RFID card with login credentials. The voting process was identical, but voters only received their receipt code on the screen; these voters could verify their ballot after the close of the election on a separate Mexican election website.

In person kiosks used at embassies and consulates

In person kiosk dashboard (Spanish)

Post Election Administration

Roughly 152,000 registered expatriate voters signed up to vote online and nearly 16,000 additional voters signed up early to vote in-person at a consulate kiosk. In all, 122,497 voted online starting the evening of May 18 through June 2. In addition, 22,243 voted in-person at an embassy or consulate on June 2, for a total of 144,740, as shown below.



2. Voter education / orientation

Prior to Election Day, from May 4-15 2024, the live election system was open for a **voter orientation period** in which citizens living overseas could log into the system and familiarize themselves with its overall operation. All the functionality of the live system was available, except for the actual ballot submission to the backend servers and the blockchain. Voters could verify their identity, onboard themselves into the system, log in, review their ballot, and practice filling out an electronic ballot. (Invitation emails and notices on the web informed voters that they were not submitting an official ballot and that voting would not be open until May 18th.) When they “submitted” a ballot, a mock voting receipt code was displayed on the screen, with the reminder stating that they had not submitted an official ballot. Also during this period, these expatriate voters could contact the election authority to correct any issue with their registrations.

In total, 40,782 expatriate voters completed onboarding during the orientation period: 66% from the United States, 4% from Canada, 3% each from Spain, Australia, and Germany, and the remaining 21% from other countries. Overall, about ⅓ of the registered online voters participated in the orientation period.

3. Election Cybersecurity and Technology

Under the hood and behind the scenes, various technologies were used to secure the Mexican election for expatriate voters. This section explains some of these technologies in order to help the reader understand how they apply to election administration and cybersecurity in our country.

In our 2023 Summer NASS paper, we mentioned a cryptographic technology called **homomorphic encryption**, which allows one to perform arithmetic on encrypted data. In particular, we used this to tally ballots for expatriate Mexican voters while ballots and totals were still encrypted. This enabled the electoral authority to report results of the expatriate voting within minutes of the close of the election and allowed voters to verify that their ballot had not been tampered with.

On a relatively nontechnical level, how does this work and why is it important?

Before the election started, an election encryption/decryption key pair was generated. The decryption key was split up using a mathematical technique called a **threshold scheme;** each member of a committee received a cryptographic portion (called a **shard**) of the key in a way that any three of them could reconstruct the key. After these shards were created, the decryption key was destroyed. This prevented potential collusion by election committee members by blocking the decryption and viewing of intermediate results. Only after the close of the election was the decryption key reconstituted.

When votes were cast, there was a programmatic check that the vote was valid and the voter generated what is called a **non-interactive zero-knowledge proof** (ZKP) of his or her vote. A ZKP is a mathematical proof that the stored, encrypted ballot has not been modified – the ballot is recorded as cast and has been tallied as recorded. After voting, each voter received a receipt code – a random string of characters – and could use this to check if his or her ballot had been altered after submission; the verification involved checking the ZKP of the ballot.

Before a ballot was officially cast, the ballot received a **blind signature** from the election server. This is a digital signature on a masked, encrypted ballot; the server checked that the ballot was from a voter who hadn't already voted and then applied a digital signature. The masking prevented anyone from pairing that ballot with a particular voter, therefore achieving voter anonymity. The voter's application removed the masked portion of the ballot and submitted the encrypted ballot with the digital signature and ZKP. The server checked each ballot submission to prove that the signature came from itself and that the ballot had not been altered in transit before storing the ballot and queuing the ballot to be included in the appropriate tally.

Encrypted ballots and encrypted contest totals were kept in separate digital lockboxes secured using the blockchain. At the close of the election, these lockboxes were downloaded and decrypted. Decrypting the totals took just a few seconds. All 144,740 anonymous ballots were decrypted in parallel, requiring a matter of minutes to complete. Result reports were generated quite quickly as a result. Subsequently, the digital signatures and ZKPs were also checked to verify the authenticity of each ballot and to confirm the totals.

4. Policy Questions

The cryptographic technology described in this section enables efficient, accurate, and secure election results. The quick reporting capability of homomorphic encryption comes with interesting questions for policy makers to consider, however. This technology encrypts each ballot, as well as the ballot totals; running tallies of each choice and contest are kept in an encrypted state from the start of the election and are not decrypted until after the election closes. Election law in many US states prohibits ballot tabulation before the election closes. Without procedural changes, intermediate results cannot be determined when the system tabulates ballots using homomorphic encryption, so might such tabulation be permitted (following the spirit of the law, rather than the letter of the law)? Could we also provide voters with receipts and allow them to perform a ZKP ballot verification as well? We hope that this section provides an adequate foundation for informed consideration of these questions.

5. Conclusions

We hope that this paper leads to some thoughtful discussion.

- For those elections allowing remote voting via the internet, could jurisdictions increase voter education and engagement with an “orientation period” for voting?
- Could jurisdictions save time and money on election administration and increase election security by using modern cryptography in elections?
- Could jurisdictions improve voter turnout overseas through electronic in-person voting at U.S. embassies and consulates? Is it worth holding a pilot at one of our consulates in Canada, for example?

6. References

- Take Me Out to the Blockchain, https://www.nass.org/node/2546, Voatz, Inc., Summer 2023 NASS Conference. This paper is a gentle introduction to the benefits of blockchains in election security and transparency.

- Voting Results of Mexicans Living Abroad (including Postal voting) https://www.votoextranjero.mx/web/vmre/inicio

- Commission for the Electoral Participation of Mexicans Living Abroad https://www.votoextranjero.mx/web/vmre/comision-de-vinculacion