Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 07 July-2024, Page No.- 4561-4570

DOI: 10.47191/etj/v9i07.27, I.F. – 8.227

© 2024, ETJ

An End to End Verifiability Proposal for the OTP-Vote Electronic Voting Model

Silvia Bast[1], Germán Montejano[2], Mario Berón[2], Paula Dieser[1]

[1]National University of La Pampa, Faculty of Exact and Natural Sciences, Uruguay 151, Santa Rosa, La Pampa, Argentina

[2]National University of San Luis, Faculty of Physical Mathematical and Natural Sciences, Ejército de Los Andes 950, San Luis, Argentina

ABSTRACT: Electronic voting systems have generated significant controversy in contemporary society due to the mistrust of the electorate. This mistrust is often rooted in the perceived inability to audit these systems with the same rigor and transparency as widely known and utilized manual voting methods. A critical requirement imposed on electronic voting systems is the capacity to ensure vote traceability without compromising voter anonymity—a complex challenge that presents significant difficulties. This study introduces an end-to-end verifiability (E2EV) proposal for the OTP Vote electronic voting model. The research examines this model through the lens of three essential criteria: individual verifiability, universal verifiability, and ballot secrecy. By analyzing these aspects, we aim to address the prevalent mistrust and contribute to the ongoing discourse surrounding the security and reliability of electronic voting systems.

KEYWORDS: electronic voting system, end to end verificability, individual verificability, universal verificability, voting secret.

1. INTRODUCTION

Technology has significantly permeated diverse societal sectors, becoming indispensable in areas such as electronic banking, virtual conferencing, online education, and collaborative content creation. Nevertheless, there remains significant mistrust regarding the adoption of electronic voting systems, primarily due to concerns about voter identity preservation and vote integrity. Unlike other digital activities, electronic voting demands anonymity and lacks a receipt for verification, requiring robust trust in the system.

In Argentina, the traditional paper-based voting system, established by the Sáenz Peña Law of 1912, involves manual processes where voters select paper ballots in a voting booth and submit them in sealed envelopes. While functioning adequately, this system is susceptible to issues such as ballot theft, result manipulation, and vote buying, leading to inefficiencies and potential electoral fraud. These drawbacks, coupled with the logistical challenges and costs associated with ballot printing, underscore the need for more advanced electoral solutions.

Electronic voting systems, defined as any vote collection involving electronic devices, offer a modern alternative. However, societal trust is crucial for their widespread acceptance. Key requirements for these systems include ballot secrecy, voter authentication, verifiability, user-friendliness, cost-effectiveness, auditability, inviolability, security, non-coercion, robustness, and scalability. Despite potential conflicts between requirements, such as verifiability and anonymity, these systems must ensure that votes are cast as intended and counted accurately.

Recent advancements in electronic voting systems have introduced additional requirements, including physical evidence for transparency, cryptographic methods for security and anonymity, software independence to detect corrupt software, and end-to-end verifiability (E2EV). E2EV allows voters to verify that their votes are correctly recorded and counted, enhancing the system's reliability and transparency.

This study is structured as follows: The subsequent section presents a review of related literature. Following this, a detailed description of the OTP-Vote Model is provided. Subsequently, the End-to-End Verifiability (E2EV) proposal is introduced and rigorously validated. Finally, the study concludes with a discussion of the findings and outlines directions for future research.

2. RELATED WORK

According to the definition by McGaley and Gibson [1], any form of vote collection that involves electronic devices can be considered an electronic voting system. It can be deduced, therefore, that there are electronic voting systems with very diverse characteristics. Some of them use electronic ballots that contain a chip on which they record the vote, which they subsequently deposit in a ballot box; finally, a machine reads the ballots to speed up the counting. Others make use of paper ballots that are marked with special pencils and then scanned at the time of vote counting. In other cases, the names of the candidates are presented on a screen so that the voter can select the one of their choice; subsequently, the vote is saved on the computer and some systems also allow the vote to be printed. In addition, there are systems that require voters to attend a polling

place while others allow remote voting. Regardless of the modality, it is important that the system presents the E2EV feature or some form of auditing, which increases the reliability of the electorate.

In the electronic voting system known as Votegrity, as presented by Chaum [2] the voter can visually verify their vote when casting it and also take home a physical receipt containing a number. After the election is closed, the voter can verify that the number on their receipt is included in the general list of votes. This system uses mixnets that prevent the traceability of votes and are part of the encryption process, and users can monitor their operation. This operation adds the E2EV feature, although it may be somewhat complex.

Ryan [3] initially proposed the Prêt à Voter system which was later developed by Chaum et al [4]. The system uses pre-printed paper ballots that consist of two parts that can be separated. On these ballots the names of the candidates are in random order. When casting the vote, the voter selects one part of the ballot and places it in the ballot box, and must destroy the other part. These ballots can be audited before the election. The fact that the ballots must be previously printed implies that they must be kept secure until the moment of use and that special care must be taken against the leakage of information from the device that prints them. In addition, special attention must be paid to the total destruction of half of the ballot, because people who enter the dark room later could reconstruct it. It could also introduce chain voting.

In [5] Fisher et al present the Punchscan system that also makes use of pre-printed ballots and proposes auditing ballots before the election, which are then discarded. After the election it allows an audit that consists of a partial random verification.

Scantegrity presented by Chaum [6], has an improved version called Scantegrity II [7] and makes use of pre-printed ballots, which are marked with an invisible ink that makes visible the code associated with the candidate voted for by a certain amount of time. This feature allows the voter to write down the code and once the election is finished, to verify that the voted code matches the one he has registered. The counting is done through optical scanning. Since the ballots are pre-printed, it must be verified that they are well formed, that they are secure, and that no information about them has been leaked at the time of printing. In the case of Scantegrity II, the user must also quickly write the code that becomes visible in a limited amount of time and must do so without errors, otherwise it could lead to future disputes.

Other systems feature homomorphic encryption, such as Adida & Rivest's Scratch & Vote [8]. In this case, the voter receives two ballots, and selects one to audit and another to cast the vote. In 2012, Benaloh et al [9] proposed the StarVote system, whose name is derived from Secure (S), Transparent (T), Auditable (A), and Reliable (R) principles. Among its principal characteristics, the system incorporates the utilization of voting machines and offers the capability of auditing and printing the vote on paper. Some systems allow remote electronic voting, among them we can mention: Helios by Adida and Adder de Kiayias et al [11].

3. THE OTP-VOTE MODEL

The full OTP-Vote model is detailed in [12] and offers unconditional anonymity and computational security that can be taken to any level required. It is based on the premise that, in relation to data, electronic voting systems must protect:

• The privacy of the voter (anonymity) indefinitely, even after the election is over, since, if an attacker obtains data from the records that maintain the relationship between the vote and the voter, they will be able to dedicate all the time to trying to decipher them.

• The security of vote data during the course of the electoral process, since afterwards the results are publicly known.

Its name is due to the One Time Pad (OTP) keys it uses and which are combined to form a single key and presents 3 stages as shown in Figure 1.

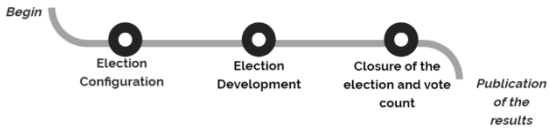

Figure 1: Model Stages

The model initially emerged as a direct application of the research carried out by García [13] in which he exposes a storage model called Multiple Channels Single Data (MSCD) (Figure. 2) which proposes dividing the total storage (T) into q channels and recording each vote once on each channel in potentially different random positions.

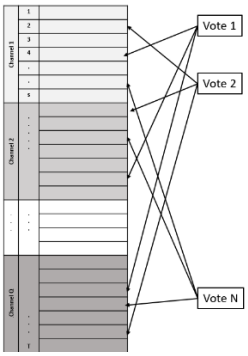

Figure 2: Multiple Channels Single Data Model

3.1 Data Components

The data components used by the model are described below.

3.1.1 One Time Pad Keys

These keys, which are an essential aspect of the system, have the following characteristics: they are random, they have the same size as the message they encrypt and from the same ciphertext, if a different key is applied, a different plaintext is obtained. They satisfy Shannon's Perfect Secrecy condition [14], that is, knowledge of the ciphertext provides no information about the original message.

3.1.2 Binary Data Files

These files store bits and are responsible for storing votes and decryption keys. They are modified during the electoral process. The model uses 2 files:

• Binary Vote File (BVF) that is modified according to the Multiple Channel Single Data (MCSD) storage model. This model proposes a solution to the Birthday Paradox [15] and García et al describe it in depth in [16]. Each of the rows or components in this file is called a tuple and can store the data of a vote and its control attributes. Figure 1 shows a simplified configuration of a tuple.

• Decryption Key (DK): It is generated from successive XOR operations (⊕) of OTP keys.

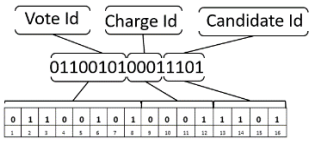

Figure 3: Basic configuration of a tuple

3.1.3 Relational Model Tables

They are tables that maintain the basic data of the election such as: positions voted, candidates, vote identifiers and flat votes that emerge after the decryption process at the end of the election.

3.2 Model Stages

The main activities carried out in each of the stages of OTP – Vote are explained in detail below.

3.2.1 Election Configuration

This stage includes the following activities:

• Establish the dimensions of the two binary files, the BVF where the votes will be stored and the DK key file, the total number of tuples T of the files must be established based on the number of channels Q that will have the BVF and the number of tuples (S) of each channel. The optimal parameter values are described in [17].

• Establish the dimensions and location of each of the attributes that will be stored as elements of the BVF (vote identifier, identifier of the voted position, Identifier of the selected candidate and control attributes). To establish these dimensions it is necessary to evaluate the probability that an intruder can detect a valid tuple among all possible tuples. As stated in [12], by increasing the redundancy in the number of bits to record each attribute, the probability of obtaining a valid tuple among all possible combinations of values can be brought to values as small as desired.

• Generation of codes for each of the identifying attributes (positions that are voted on, candidates and Vote identifiers), which must comply with the set of requirements specified in [18].

• Generation of the tables: Vote Identifiers, Voted Positions, Candidates, taking into account the specifications previously established about the dimensions and location of the attributes.

• As the last activity of the stage, the presence of the Electoral Authorities (EA) is required, which will provide two keys each, one K_{i1} which will provide the initial values to BVF and another K_{i2} which will initialize the DK. This process makes use of the XOR (⊕) operation through the following formulas:

$$BFV = BFV \oplus K_{i1} \forall i, 1 \le i \le EA \quad (1)$$

$$DK = DK \oplus K_{i2} \forall i, 1 \le i \le EA \quad (2)$$

In the first equation, the initial values are given to BVF, and in the second to the DK through the through the contributions of the keys of each EA.

3.2.2 Election Development

This stage consists of two clearly differentiated moments:

• The authentication of the voter.

• The casting of the vote.

The first process consists of verifying that the voter is included in the list of qualified voters. To carry out this activity, the voter registers at the election site with the electoral authorities, proving their identity by presenting their identification.

If sufficient resources were available, authentication could be used through biometric data, such as fingerprints, voice, retina. The separation of the authentication and vote casting processes is an important contribution to the anonymity characteristic of the vote, since it prevents the relationship between the vote and the voter who casts it from being recorded.

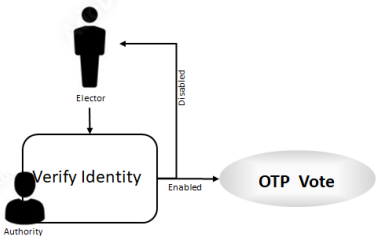

Figure 4: Authentication Process

Once the voter is authenticated, he moves forward to the vote casting process. In this stage, the MCSD storage model is used (Figure 2). For each vote v the process detailed below will be carried out.

The electoral official at the polling station verifies the voter's registration status before granting authorization to enter the voting booth. Once inside, the voter selects their preferred candidate(s). This selection is converted into a bit string (BitString) that serves as input to the vote casting process.

On the other hand, the system must:

• Randomly obtain a valid Vote Identifier (VoteId) for vote v.

• Generate the following data:

– The Initial contribution of the vote ($InitialContribution_v$), which consists of a string of zeros of the same dimensions as the BVF and the DK.

– The set of random numbers SetQ ={q_i} such that 1<=i<=S for each of the Q channels, where q_i represents the place

where the vote will be stored on the ith-channel. The cardinality of SetQ is Q.

– Random vote key called $VoteKey_v$, and which has the same dimension as the BVF and the DK.

The system combines the VoteId that was randomly taken from the Vote Identifiers table that was generated before the start of the election process and combines it with the BitString that comes from the user's election.

This combination is developed according to the parameterization that was carried out in the election configuration stage. From this process the $VoteChain_v$ emerges. Once the $VoteChain_v$ is generated, the system proceeds to combine it with the $InitialContribution_v$, taking into account the positions indicated in the SetQ, as shown in Figure 5. To achieve this combination, the XOR of the $VoteChain_v$ is carried out with the slots or rows corresponding to each of the q_i of the Initial $Contribution_v$, being generated in this way, the $Contribution_v$.

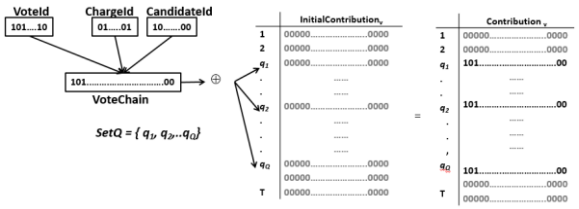

Figure 5: $Contribution_v$ generation process

Once the $Contribution_v$ is produced, it is combined with the $VoteKey_v$ to obtain the $FinalContribution_v$.

$$FinalContribution_v = Contribution_v \oplus VoteKey_v \quad (3)$$

In this way the vote is encrypted. The process can be seen in the Figure 6.

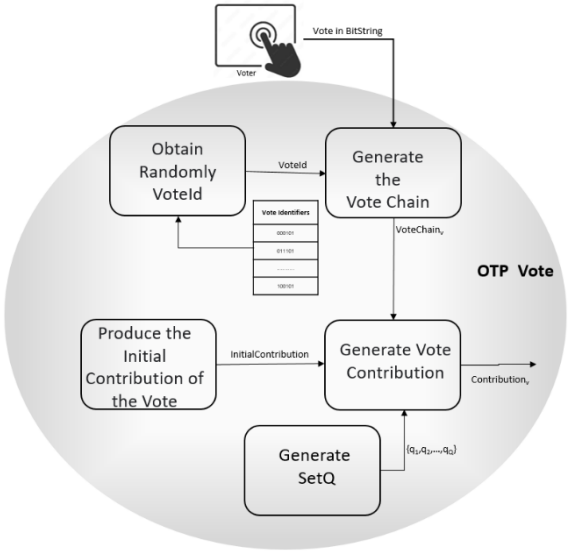

Figure 6: Generate contribution

The encrypted vote is then stored in the BVF. To do this, the following operation is carried out:

$$BVF = BVF \oplus FinalContribution_v \quad (4)$$

Finally, the $VoteKey_v$ is used to update the DK, using the following operation:

$$DK = DK \oplus VoteKey_v \quad (5)$$

The entire voting process is observed in the Figure 7.

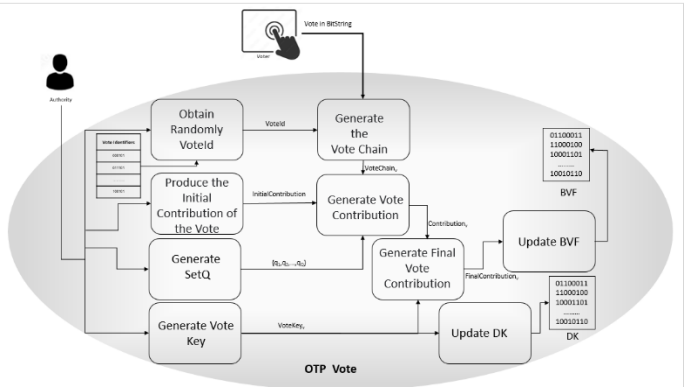

Figure 7: Vote Casting Process

Once the BVF and the DK have been updated, the vote cast advice reaches the electoral authority and the voting booth is available so that another person can be enabled to vote.

3.2.3 Closure of the Election and Vote Count

At this point, the presence of the electoral authorities is required again.

The vote decryption process consists of three sub processes:

- Application of Key 1 of the Authorities to the latest version of the BVF (Formula 1).
- Application of Keys 2 of the Authorities to the latest version of the DK. (Formula 2).
- XOR between the BVF and the DK resulting from the previous steps.

For these purposes, it is once again required that each of the authorities provide the initial keys that were stored in a secure place and the following operations are applied:

Finally to obtain the Decrypted Vote Binary File (DBVF) the following is applied:

$$DBVF = BVF \oplus DK \quad (6)$$

Once the DBVF is obtained, the votes are retrieved and counted, as specified in [19]. Finally, the results and the Flat Votes table are published. The complete process of closing the election and counting votes can be seen in Figure 8.

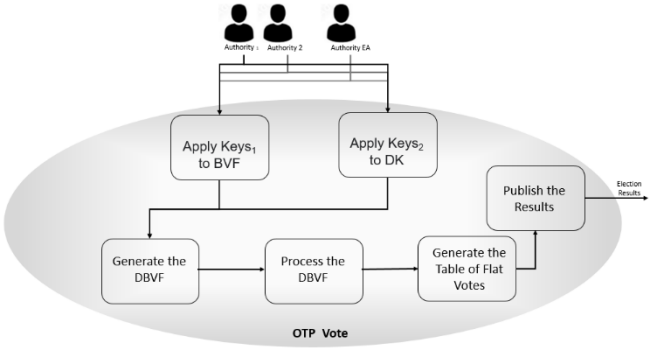

Figure 8: Closing of the Election and Counting of Votes

.

4. END TO END VERIFIABILITY FOR THE OTP-VOTE MODEL

According to Benaloh et al. [20], an electronic voting system must satisfy two key criteria to achieve end-to-end verifiability (E2EV): i)"Cast as intended": Voters must be able to verify that their votes are accurately recorded in accordance with their intentions. ii)"Counted as cast": Any member of the public should be able to verify that each recorded vote is correctly included in the final tally.

A simple way to meet these requirements would be to publish the list of each voter with the vote cast, that way, everyone could verify that the votes were recorded correctly and that the final count coincides exactly with the published results. But, given the anonymity characteristic that electronic voting systems must comply with, this methodology is not applicable.

It is clear then, that for a system to present E2EV it must meet the following requirements:

- Individual verifiability: any voter can verify that their vote was included in the count.
- Universal verifiability: Anyone can determine that the total vote count is correct.
- Voting secrecy: no voter will be able to prove who they voted for.

Taking into account the requirements of E2EV and the operation of the original OTP - Vote model, the following E2EV proposal is presented.

Once the voter has registered, entered the dark room and selected the candidate of their preference, the system, in addition to obtaining a random VoteId, will generate a large random number (LN), on which it will apply a function f that will produce a result H, that is, f(LN)=H.

This H value will be added as a new attribute to each vote. That is, each tuple will now be made up of the attributes of the vote, the control bits and H. In the election configuration stage, the number of bits to be allocated H and their location within the tuple must also be taken into account. When the vote is stored, the resulting H value is also stored.

Once the user has cast their vote, the system prints:

- The paper vote: which the user will deposit in the ballot box when he or she leaves the dark room;
- A large random number (LN) that the voter will take with him.

When the time allocated for casting votes ends, the election is closed and the votes are counted. As expressed in the Closure of the Election and Vote Count section, the BVFD is generated and the flat votes and also the H values that were stored with them are obtained.

After the counting is completed and the results published, it will also be published on the site of election:

The list of votes with their corresponding H values. It should be noted that the list of votes is displayed in the random order in which they were stored.

- The list of LN.
- The function f that was applied on the LN to produce the values of H.

The idea behind publishing the aforementioned information is to allow voters to audit the results.

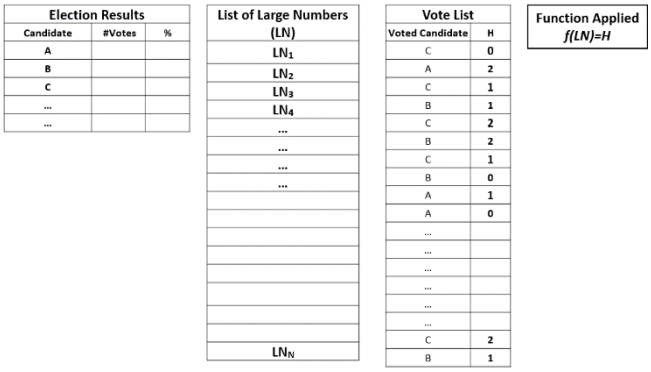

Figure 9: Result of the election and Elements that Facilitate Audit

Each voter will be able to:

- Verify that the LN that the system issued and that he or she has in his or her possession is included in the LN List.
- Apply the function f to his or her own LN (or any of the LN that were published) to determine the result H.
- Observe the values of H that are stored in each tuple that represent a vote.
- Check that the quantity of LN published coincides with the number of voters registered at the polling station.
- The total quantity of results of the function f must also equal the number of votes cast.

Based on the analysis of the proposal in light of the three requirements that the system must meet to ensure E2EV, a scenario was detected in which voting secrecy would be threatened. The case in question is shown in Figure 11, in which it can be seen that a single voter, by applying the function f on his LN, has obtained the value of H = 2, then that voter could prove to third parties that he voted for candidate A.

Based on the situation presented, progress was made in the empirical study of the different quantities of discrete values (D) that the function H can return, taking into account the number of voters (N) assigned to a given voting table.

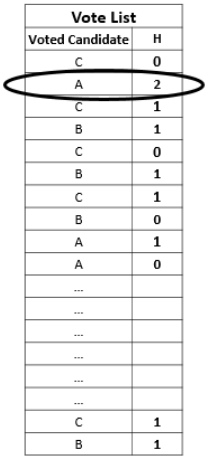

Figure 11: Unwanted Case

After developing simulations of assigning random values to voters and performing probability calculations evaluating the quantity of unwanted cases over the quantity of possible cases for different values of D and N, [21] advances the following conclusions:

- 100,000 simulations were carried out and no "unwanted cases" were presented.
- The distribution that appears most frequently in terms of discrete results corresponds to N/D. As an example, if the function f returns 3 different values H_0, H_1 and H_2 and there are registered N=300 votes, the combination that was presented with the highest frequency was N/D, this is 300/3 which indicates that 1/3 of the voters received the value 0 as a result of the function f on their LN, 1/3 the value 1 and 1/3 the value 2.
- Smaller values of D would show better performance in relation to "unwanted cases".

Taking these results into account, progress was made in obtaining a formula that would allow obtaining the probability of an unwanted case occurring. For this purpose, a polling station of N voters is considered.

Let f(LN) be the function that assigns each voter one of the values H ∈{ 0, 1, 2} randomly. Therefore, for any voter:

$$P(H=0)=P(H=1)=P(H=2)=1/3 \quad (7)$$

It is also assumed that assignments are made independently.

Under these assumptions, the random variable is defined for each H ∈ {0, 1, 2}:

X_H = "number of voters, among N, who receive the value H".

Then $X_H \sim Bi(N;\frac{1}{3})\ \forall\ H \in \{0, 1, 2\}$

The random vector X = (X_0, X_1, X_2) is now considered.

Then $X \sim M(\frac{1}{3};\frac{1}{3};\frac{1}{3})$

It is important to calculate the probability of the event:

S = "there is any identifiable voter at the electoral table".

This happens in one of the following two cases:

A = "a single voter is identifiable".

B = "two voters are identifiable"

Therefore S = A ∪ B being A ∩ B = ∅. Then:

$$P(S) = P(A \cup B)=P(A)+P(B) \quad (8)$$

It is calculated now P(A). A occurs when any of the A_H events occur H ∈ {0, 1, 2} defined as: A_H = "the identifiable person received the value H".

Then

$$P(A)= P(A_0 \cup A_1 \cup A_2) = P(A_0)+P(A_1)+P(A_2) \quad (9)$$

This equality is valid because each person receives a single value, which then corresponds to mutually exclusive events.

$$P(A_0)+P(A_1)+P(A_2)=3P(A_0) \quad (10)$$

This equality holds because the events AH are equiprobable.

It is then calculated $P(A_0)$.

Note that A_0 occurs in one of the cases A_{01}, A_{02} or A_{03}, which are defined below, all of which are incompatible two by two:

$$A_{01} = \bigcup_{k=2}^{n-3} A_{0k} \quad (11)$$

Where $A_{0k} = (X_0=1) \cap (X_1=k) \cap (X_2 =N-(k+1))$

$$A_{02} = (X_0 =1)\cap(X_1 =0)\cap(X_2 =N-1) \quad (12)$$

$$A_{03} = (X_0 =1)\cap(X_1 =N-1)\cap(X_2 =0) \quad (13)$$

Then $A_0 = A_{01} \cup A_{02} \cup A_{03}$.

Therefore

$P(A_0) = P(A_{01} \cup A_{02} \cup A_{03}) = P(A_{01}) + P(A_{02}) + P(A_{03})$

Each probability is calculated separately.

$$P(A_{01}) = P(\bigcup_{k=2}^{N-3} A_{0k}) = \sum_{k=2}^{N-3} P(A_{0k}) \quad (14)$$

$$= \sum_{k=2}^{N-3} \frac{N!}{1!k!(N-(k+1))!}\left(\frac{1}{3}\right)^1\left(\frac{1}{3}\right)^k\left(\frac{1}{3}\right)^{N-(k+1)} \quad (15)$$

$$= \sum_{k=2}^{N-3} \frac{N!(N-k)}{k!(N-k)!}\left(\frac{1}{3}\right)^N \quad (16)$$

Then

$$= \sum_{k=2}^{N-3} \binom{N}{k}(N-k)\left(\frac{1}{3}\right)^N \quad (17)$$

$$P(A_{02}) = \frac{N!}{1!0!(N-1)!}\frac{1}{3}^1\frac{1}{3}^0\frac{1}{3}^{N-1} = N\frac{1}{3}^N \quad (18)$$

$$P(A_{03}) = \frac{N!}{1!(N-1)!0!}\frac{1}{3}^1\frac{1}{3}^{N-1}\frac{1}{3}^0 = N\frac{1}{3}^N \quad (19)$$

Then

$$P(A_0) = \sum_{k=2}^{N-3} \binom{N}{k}(N-k)\left(\frac{1}{3}\right)^N + 2N\left(\frac{1}{3}\right)^N \quad (20)$$

$$\left[\left(\sum_{k=2}^{N-3} \binom{N}{k}(N-k)\right)+2N\right]\left(\frac{1}{3}\right)^N \quad (21)$$

Hence

$$P(A) = 3P(A_0) \quad (22)$$

$$= 3\left[\left(\sum_{k=2}^{N-3} \binom{N}{k}(N-k)\right)+2N\right]\left(\frac{1}{3}\right)^N \quad (23)$$

$$= \left[\left(\sum_{k=2}^{N-3} \binom{N}{k}(N-k)\right)+2N\right]\left(\frac{1}{3}\right)^{N-1} \quad (24)$$

Now P(B) is calculated. Note that B occurs in one of the following cases (two-by-two incompatible).

B_{01} = (X0 = 1) ∩ (X1 = 1) ∩ (X2 = N − 2)
B_{02} = (X0 = 1) ∩ (X1 = N − 2) ∩ (X2 = 1)
B_{03} = (X0 = N − 2) ∩ (X1 = 1) ∩ (X2 = 1)

Then, B = B_{01} ∪ B_{02} ∪ B_{03}
Therefore: P(B) = P(B_{01} ∪ B_{02} ∪ B_{03})
= P(B_{01}) + P(B_02) + P(B_{03}) = 3P(B_{01})

$$P(B_{01}) = \frac{N!}{1!1!(N-2)!}\left(\frac{1}{3}\right)^1\left(\frac{1}{3}\right)^1\left(\frac{1}{3}\right)^{N-2} \quad (25)$$

$$= N(N-1)\left(\frac{1}{3}\right)^N \quad (26)$$

Then

$$P(B) = 3P(B_0) = 3N(N-1)\left(\frac{1}{3}\right)^N \quad (27)$$

$$== N(N-1)\left(\frac{1}{3}\right)^{N-1} \quad (28)$$

Finally, to obtain P(S), as established in Formula 8, Formulas 24 and 28 are added.

$$P(S) = \left[\left(\sum_{k=2}^{N-3}\binom{N}{k}(N-k)\right) + 2N + N(N-1)\right]\left(\frac{1}{3}\right)^{N-1} \quad (29)$$

$$P(S) = \left[\left(\sum_{k=2}^{N-3}\binom{N}{k}(N-k)\right) + N^2 + N\right]\left(\frac{1}{3}\right)^{N-1} \quad (30)$$

Applying the formula it is possible to obtain the probability of "there is some identifiable voter among N voters" for a function with D = 3.

Analogously, for the same event, now thinking of 4 discrete results (D=4), the following cases could be presented:

A = "a single voter is identifiable".
B = "two voters are identifiable".
C = "three voters are identifiable".

Following each of the cases, the final formula would be expressed as follows.

$$P(S) = P(A \cup B \cup C) = P(A) + P(B) + P(C) \quad (31)$$

Where

$$P(A) = \frac{N!}{4^{N-1}}(a1 + a2 + a3) \quad (32)$$

$$a1 = \sum_{k=2}^{N-5}\sum_{m=2}^{N-3-k}\frac{1}{k!m!(N-(1+k+m))!} \quad (33)$$

$$a2 = 3\sum_{k=2}^{N-3}\frac{1}{k!(N-(1+k))!} \quad (34)$$

$$a3 = \frac{3}{(N-1)!} \quad (35)$$

$$P(B) = \left(\sum_{k=2}^{N'4}\frac{N!}{k!(N-(2+k))!} + 2\frac{N!}{(N-2)!}\right) + \frac{1}{4}^N 6 \quad (36)$$

$$P(C) = N(N-1)(N-2)\frac{1}{4}^{N-1} \quad (37)$$

Applying Formula 31, it will be possible to obtain the probability of "there is some identifiable voter among N voters" for a function with D = 4

In this way it was possible to specify the formulas that allow determining the probability that among all the votes someone can be identified, that is, that the secrecy of the vote is broken, for 3 and 4 discrete values.

5. VALIDATION OF THE E2EV

For the system to comply with the VE2E property, it must provide: individual verifiability, universal verifiability and must present the characteristic of anonymity or voting secrecy. The following details how the E2EV proposal for OTP Vote covers the three aforementioned aspects.

Individual Verifiability

At the end of the election and after the data is published, each voter will be able to verify that the LN that the system issued and that he or she has in his or her possession, is included in the Public List of LN. It will also be possible to apply the function f on the LN to obtain the H and verify that a pair exists in the list (H, Voted Candidate).

3.3 Universal Verifiability

The quantity of LN numbers published must match the quantity of registered voters at the polling station. And the total number of results of the function f must also be equal to the number of votes cast. Furthermore, since all LNs are published, anyone could apply the function to each of them and verify that the results of H match for all votes.

Voting Secrecy

Applying the formulas obtained for D=3 and D=4, which responds to the probability that among N voters there is one that can be identified, the results shown in Table 1 are obtained

Table 1 Probability that among N Voters there is One Who can be Identified for D=3 y D=4

N	Probability P(S) D= 3	Probability P(S) D= 4
100	3,69E-16	4,27E-11
200	1,81E-33	2,74E-23
250	3,56E-42	16E-71
300	6,70E-51	6,60E-86
350	1,23E-59	7,99E-101

The table shows values of N that range between 100 and 350, and it can be seen that the decrease in the probability that the secrecy of the vote can be broken presents positive although negligible values. It should also be taken into account that as the value of N increases, the probability of breaking the voting secrecy decreases. The N values take in count that in Argentina there are between 250 and 350 voters assigned to each polling station.

6. CONCLUSION

The work presents an E2EV proposal for the OTP Vote model and evaluates its behavior through the analysis of each of the 3 characteristics: Individual Verifiability, Universal Verifiability and Vote Secrecy. From the study it emerges that the model behaves adequately for the first two requirements, but presents a potential problem for compliance with voting secrecy. From the analysis of the amount D of possible discrete results for H that the function f returns, it is found that small values of D present better results.

Progress was then made in obtaining the formulas that allow calculating the probabilities that the voting secrecy could be broken for a function with D = 3 and D = 4. It was observed that the formulas respond adequately, significantly decreasing the probability that the secrecy of the vote can be broken as the number of voters increases. By applying the formulas to different values of N, it is concluded that the model behaves in a very acceptable manner, given that for polling stations with 300 voters (which presents the average number of voters assigned to a position in Argentina), the probability , shows 51 zeros in front of the first significant digit, which leads to the conclusion that the probability presents negligible values, which could also be reduced even more, if 2 polling stations were grouped together, reaching 600 voters, or 3 polling stations, which It would reach a number of 900 voters, that is, the probability can be reduced as much as desired.

As future work, it remains to continue advancing in the generalization of the formula for different values of D and to deepen the exhaustive evaluation of the proposal with the objective of demonstrating results that increase the confidence of the electorate.

REFERENCES

1. M. McGaley & J. Gibson, "A critical analysis of the council of Europe recommendations on e-voting", In Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop EVT'06, USENIX Association, pp. 1–13, 2006.
2. D. Chaum, "Secret-ballot receipts: True voter-verifiable elections", IEEE Security & Privacy, 2(1), pp 38–47, 2004.
3. P. Ryan, "A variant of the Chaum voter-verifiable scheme". In Proceedings of the 2005 Workshop on Issues in the Theory of Security pp. 81-88, 2005.
4. D. Chaum, P. Ryan & S. Schneider. "A practical voter-verifiable election scheme". In Computer Security–ESORICS 2005: 10th European Symposium on Research in Computer Security. Proceedings 10 (pp. 118-139). Springer Berlin Heidelberg. 2005.
5. K. Fisher, R. Carback, & A. Sherman. "Punchscan: Introduction and system definition of a high-integrity election system". In Proceedings of Workshop on Trustworthy Elections, pages 19–29, 2006.
6. D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman & P. Vora, P., "Scantegrity: End-to-end voter-verifiable optical-scan voting". IEEE Security & Privacy, 6(3), 40-46, 2008.
7. D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. Rivest, P. Ryan, E. Shen, A. Sherman & P. Vora, "Scantegrity II: End-to-end verifiability by voters of optical scan elections through confirmation codes". IEEE transactions on information forensics and security, 4(4), 611-627, 2009.
8. B. Adida & R. Rivest. "Scratch & vote: self-contained paper-based cryptographic voting". In Proceedings of the 5th ACM workshop on Privacy in electronic society. pp. 29-40, 2006.
9. J. Benaloh, M. Byrne, P. Kortum, N. McBurnett, O. Pereira, P. Stark & D. Wallach, D., "STAR-Vote: A secure, transparent, auditable, and reliable voting system". arXiv preprint arXiv:1211.1904, 2012.
10. B. Adida, "Helios: Web-based Open-Audit Voting". In USENIX security symposium. Vol. 17, pp. 335-348, 2008.
11. A. Kiayias, M. Korman and D. Walluck, "An Internet Voting System Supporting User Privacy", In 22nd Annual Computer Security Applications Conference (ACSAC'06), pp. 165-174, 2006.
12. S. Bast, S, Confidencialidad e Integridad de Datos en Sistemas de E-Voting: un Modelo para la Implementación Segura de un Sistema de Voto Electrónico Presencial. Editorial Académica Española. 2017.
13. P.García, J. van de Graaf, G. Montejano, S. Bast & O. Testa, "Implementación de canales paralelos en un protocolo Non Interactive Dining Cryptographers". In XLIII Jornadas Argentinas de Informática e Investigación Operativa (43JAIIO)-VI Workshop de Seguridad Informática. pp 1-15, 2014.
14. C. Shannon, "Communication theory of secrecy systems". The Bell system technical journal, 28(4), 656-715, 1949.
15. P. García, J. van de Graaf, A. Hevia & A. Viola, "Beating the birthday paradox in dining cryptographer networks". In Progress in Cryptology-LATINCRYPT 2014: Third International Conference on Cryptology and Information Security in Latin America. Revised Selected Papers 3 (pp. 179-198). Springer International Publishing (2015).
16. P. Garcia, J. van de Graaf, G. Montejano, D. Riesco, N. Debnath and S. Bast, "Storage Optimization for Non

Interactive Dining Cryptographers (NIDC)". In 12th International Conference on Information Technology - New Generations, pp. 55-60, 2015

17. P. García, S. Bast, E. Fritz, G. Montejano, D. Riesco & N. Debnath, "A systematic method for choosing optimal parameters for storage in parallel channels of slots". In 2016 IEEE International Conference on Industrial Technology (ICIT), pp. 1700-1705, 2016.
18. S. Bast, P: García, G. Montejano, "Generación de Códigos para OTP Vote". In 5º Congreso Nacional de Ingeniería Informática/ Sistemas de Información (CoNaIISI). ISSN: 2347-0372. pp. 12-22. (2017)
19. P. García, S. Bast & G. Montejano, "Recuento y recuperación de sufragios en OTP–Vote". In XI Simposio Argentino de Informática en el Estado (SIE)-JAIIO 46 pp 38-51 (2017).
20. .J. Benaloh, R. Rivest, P. Ryan, P. Stark, V. Teague, & P. Vora, P. (2015). "End-to-end verifiability". arXiv preprint arXiv:1504.03778 (2015).
21. S. Bast, G. Montejano, M. Berón, "Verificabilidad End to End y Secreto de Voto en el Modelo OTP – Vote". In 10 º Congreso Nacional de Ingeniería en Informática / Sistemas de Información, (CoNaIISI). ISBN 978-950-42-0218-9. . pp. 534-544. (2022)