David Chaum's Voter Verification using Encrypted Paper Receipts

Poorvi Vora

In this document, we provide an exposition of David Chaum's voter verification method [1] that uses encrypted paper receipts.

1 Players

We assume the following players:

1. The **Voter** should be able to determine that her vote is counted and anonymous.

2. The **Polling Station** is responsible for (a) recording the voter's vote, while ensuring that it is not possible to thereafter link a particular vote with a voter, (b) ensuring that exactly one vote is cast by each voter and (c) that only legitimate voters vote. The system must catch attempts by the Polling Station to change votes.

3. **Trustees** are responsible for ensuring that the votes are counted and anonymous. This role is played out in physical elections by some combination of candidate representatives and government officials, depending on the country. An election must not be cleared in the presence of cheating trustees, unless all trustees cheat.

4. **Interested Third Parties** may verify that the system is working as it should. This role is played out by organizations such as League of Women Voters in physical elections in the US. The method described in this document requires the participation of Interested Third Parties, as their participation is the only way to detect attempts by the Polling Station to change votes.

5. **Auditor** or **Certification Authority** certifies that the election results are correct and have been determined as originally specified. Who the Auditor is depends on who the results are being certified for. In physical elections in the US this role is played by a specified government/judicial official. In physical elections in some countries like India, this role is played by a citizen who is not answerable to the Parliament and hence is more independent of the current office bearers. In physical elections in new democracies, this role is played by

organizations like Amnesty International who may also function as Interested Third Parties. In the method described in this document, exactly one audit is possible. More audits will compromise voter anonymity.

6. The **Public**, represented by the public site that holds all receipts, trustee decrypted receipts, and audit results, and displays them to the public, thus enabling anyone to count the votes and follow the vote verification process.

The voting process has the following additional requirements not mentioned above:

1. **Involuntary Privacy** No voter should be able to prove to a third party how she voted.
2. **Election Validity** It should not be possible to forge a receipt or in any other way falsely call into question the validity of an election.

Note: Voter authentication is not discussed in this document. Hence, ballot stuffing, false electoral rolls, and the separation between voter and assigned ballot card would have to be addressed through different means. The security of cast ballots is also not discussed, hence other methods need to be used to ensure that the Polling Station does not retain the entire vote and associate it with a serial number.

2 Sketch of method without technical details

1. The voter casts a vote electronically and is given opportunities to change and confirm the vote. Once it is confirmed, the polling station prints two overlaid layers, each a random binary image. Together, these two images provide a visual representation to the voter of her choices as recorded by the system. This representation is the equivalent of a filled-in paper ballot. In addition to the binary image there are three numeric strings at the bottom of the layers, the strings identical on both layers. These strings force the Polling Station to commit to the seeds used to generate the random pixels on the two layers, and help detect efforts by the Polling Station to change votes.

2. The voter checks that her votes are recorded as cast, and that the three numeric strings are identical on both layers. She then chooses the layer she wishes to take with her as a receipt. The chosen layer is an encrypted visual representation of her vote. The other layer may be thought of as the decryption key, and is destroyed by the Polling Station (there is no way to ascertain this). The three numeric strings contain encrypted information on generating the decryption key. This information can be decrypted with the participation of all trustees. Before the voter leaves with her receipt, the Polling Station prints some more information. This information certifies that the

receipt is authentic and allows anyone to check that the random pixels on the chosen layer were correctly generated.

3. Outside the Polling Station or before a certain pre-determined deadline, the Interested Third Parties and voters themselves can check that (a) the random numbers on the chosen layer were correctly generated, (b) half of the information encrypted for the trustees is correct, and (c) that the receipt is legitimate. For each vote checked, the Polling Station's attempt to change the vote can be detected with probability $\frac{1}{2}$. To change the outcome of an election the Polling Station would need to change a large number of votes, and to detect cheating by the Polling Station, enough of the votes would need to be thus checked. The Public website displays all collected ballots by serial number. Individual voters or Interested Third Parties may check that particular votes are among these. Again, for confidence in the result, a large enough fraction of the votes cast must be thus checked to detect attempts by the Polling Stations to destroy some votes. Any anomalies would provoke further checks to determine the extent of the problem (a faulty machine, Polling Station, District, etc.).

4. The votes are decrypted by the trustees to produce the filled-in ballot images approved by the voters. Each vote is stripped off everything except the image and the numeric strings required to generate the decryption key. Each trustee performs his part of the decryption on the image and passes it on to the next trustee after shuffling the entire set of images. The set of input and output images for each trustee are publicly available. The shuffle prevents the linking of a final decrypted ballot image with a serial number and through that with a particular voter. The final trustee produces ballots which are displayed on the website and counted. All trustees retain the shuffle used for the audit. A trustee can cheat in two ways: by not shuffling correctly, or by not decrypting correctly. Through an audit, both may be detected with probability $\frac{1}{2}$ for each vote cheated on.

5. The audit involves requiring each trustee to demonstrate publicly the output image corresponding to specified input images. The specified images are chosen at random, and number half of the total number of input images. The correspondence between the two images may be checked using the trustee's public key. Specified input images for consecutive trustees are chosen so that no final ballot image can be linked to a serial number, as this would compromise voter anonymity.

3 Keys held by various players

Some of the players are required to use their public/private key pairs. If K represents the key pair, K_{pub} and K_{priv} represent the public and private keys respectively. We assume an existing PKI: all private keys are securely held, and all public keys freely available and appropriately certified. The use of these key pairs makes the system vulnerable to any known security problems with PKIs.

The following will be the assumed key pairs:

1. K_i: key pair for the i^{th} trustee, a total of N trustees
2. o_t: Polling Station key pair for signing the entire receipt, top layer
3. o_b: Polling Station key pair for signing the entire receipt, bottom layer
4. s_t: Polling Station key pair for generating that half of the random image embedded in top layer
5. s_b: Polling Station key pair for generating other half of the random image

Additional Notation:

q: serial number

$S_K(x)$: digital signature of x using public key pair K, or encryption of a specified digest of x using K_{priv}

4 More Details: At the polling station

Step 1: *The voter chooses his candidates using a UI i.e. voter defines the filled-in ballot, binary image $B(q)$*

For example, $B(q)$ could be:

$$B(q) \quad = \quad \begin{matrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix}$$

representing, say, candidate 2.

Step 2: *Polling Station generates a random image and its complement such that the two images, when overlayed, provide a pictorial representation of the voter's choices, image $B(q)$.*

Say $W(q)$ is a randomly generated image, and $R(q) = W(q) \oplus B(q)$ the Complement Image. For example,

$$W(q) \quad = \quad \begin{matrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{matrix} \qquad\qquad R(q) \quad = \quad \begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$$

Note that $B(q) = W(q) \oplus R(q)$

See section 4.2.2 for details on generating $W(q)$.

4.1 Aside: A bad choice of receipt

Note that both $R(q)$ and $W(q)$ are random by themselves, and each can be thought of as an encrypted version of $B(q)$ with the other as the key. The voter could match the layer she holds with a set of votes being “counted”, however she cannot check the key used to decrypt that layer. The polling station could change the key (other layer), and thus her vote. If the voter always walked away with one, say A, the polling station could print a layer C such that $B(q) = A \oplus C$. This layer will never be used again. The voter will assume it is to be used in the process, while the key used to decrypt the vote is Fake Layer = Fake Vote $\oplus$ A. For example, if the voter walked away with layer $R(q)$, the Polling Station would print $W(q)$ so that the voter sees $B(q)$, but use Fake Layer for decryption:

$$\text{Fake Layer} \quad = \quad \begin{array}{cccc} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}$$

so that Fake Vote = Fake Layer $\oplus$ $R(q)$ is

$$\text{Fake Vote} \quad = \quad \begin{array}{cccc} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{array}$$

which can be thought of as representing Candidate 3.

4.2 Pixel Swapping

To thwart this, alternate pixels of the two layers are swapped, still maintaining the XOR of their values, and hence the value of the vote. The voter is allowed to choose the layer she leaves with.

Step 3: *Alternate pixels of the random and complement images are swapped to create a top and bottom layer*

We demonstrate with an example before specifying the technicalities.

4.2.1 Example

For example, $W(q)$ with even-numbered pixels in odd-numbered rows and odd-numbered pixels in even-numbered rows swapped with $R(q)$ becomes $L_t(q)$, the Top Layer:

$$W(q) \quad = \quad \begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array} \qquad R(q) \quad = \quad \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \qquad L_t(q) \quad = \quad \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}$$

Similarly, $W(q)$ with odd-numbered pixels in odd-numbered rows and even-numbered pixels in even-numbered rows swapped with $R(q)$ becomes $L_b(q)$, the Bottom Layer:

$$L_b(q) \quad = \quad \begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}$$

Note that $L_t(q) \oplus L_b(q) = W(q) \oplus R(q) = B(q)$. The random values in $L_t(q)$ are denoted $W_t(q)$ and are generated using key s_t.

$$W_t(q) \quad = \quad \begin{array}{cccc} 0 & - & 0 & - \\ - & 0 & - & 1 \\ 1 & - & 0 & - \\ - & 1 & - & 1 \end{array}$$

The random values in $L_b(q)$ are denoted $W_b(q)$ and are generated using key s_b.

$$W_b(q) \quad = \quad \begin{array}{cccc} - & 1 & - & 0 \\ 1 & - & 0 & - \\ - & 1 & - & 0 \\ 0 & - & 0 & - \end{array}$$

4.2.2 In Technical Terms

The above swapping is the reason why $W(q)$ is generated as two sequences of random numbers. It consists of alternate pixels of $W_t(q)$ and $W_b(q)$, where

$$W_c(q) = \sum_i^N h'(h(i, S_{s_c}(q)) \tag{1}$$

where c represents either t or b, the sum is over all trustees, and h' and h are public one-way functions or PRNGs (pseudo-random number generators).

Suppose $2n$ is the number of columns of the binary image, and that $\lceil x \rceil$ represents the smallest integer greater than or equal to x (ceiling(x)). If the $(i,j)^{th}$ pixel of image $I(q)$ is denoted $I(q,i,j)$, and numbering begins from $i = 1$ and $j = 1$, then, for even $i + j$

$$L_t(q,i,j) = W_t(q,(i-1) \times n + \lceil \frac{j}{2} \rceil) \tag{2}$$

and for odd $i+j$:

$$L_t(q,i,j) = W_b(q,(i-1)\times n + \lceil \frac{j}{2} \rceil) \oplus B(q,i,j) \tag{3}$$

Similarly, for even $i+j$

$$L_b(q,i,j) = W_t(q,(i-1)\times n + \lceil \frac{j}{2} \rceil) \oplus B(q,i,j) \tag{4}$$

and for odd $i+j$:

$$L_b(q,i,j) = W_b(q,(i-1)\times n + \lceil \frac{j}{2} \rceil) \tag{5}$$

4.3 Communicating the random values to the trustees

Step 4: *Encrypted values of the random number seeds are printed at the bottom of both layers, along with the registration number.*

Again, we illustrate with an example before describing the technical detail.

4.3.1 Example

If the voter chooses the bottom layer, $L_b(q)$, the top layer, $L_t(q)$ is discarded at the booth. For decryption of the retained layer $L_b(q)$, the trustees need to be able to determine $L_t(q)$, or at least $W_t(q)$, so that they may determine $L_b(q,i,j) \oplus W_t(q,(i-1)\times n + \lceil \frac{j}{2} \rceil) = B(q,i,j)$ for even $i+j$ (see equation (4)). From equation (5) it is clear that there is no information about the vote contained in $L_b(q,i,j)$ for odd $i+j$, and $B(q,i,j)$ cannot be determined for odd $i+j$ from only $L_b(q)$.

In our example, if the trustees had the random values of the top layer they could construct:

$L_b(q)$				$\oplus$	$W_t(q)$				$=$	$B(q)$			
0	1	0	0	$\oplus$	0	-	0	-	$=$	0	-	0	-
1	1	0	1		-	0	-	1		-	1	-	0
1	1	0	0		1	-	0	-		0	-	0	-
0	0	0	1		-	1	-	1		-	1	-	0

4.3.2 Technical Details

To provide the random values, two “dolls”:

i. $\mathcal{D}_t^N$, encrypted information to generate random values in the top layer, $W_t(q)$

ii. $\mathcal{D}_b^N$, encrypted information to generate random values in the bottom one, $W_b(q)$

are printed at the bottom of both layers along with registration number q.

$\mathcal{D}_t^N$ and $\mathcal{D}_b^N$ are computed recursively, starting with the first doll, which contains encrypted information for the first trustee.

$$\mathcal{D}_c^1 = K_{1_{Pub}}[h(1, S_{s_c}(q)); empty_doll] \tag{6}$$

where c represents t or b. The i^{th} doll and information required for the next trustee are locked together inside the $(i+1)^{th}$ doll :

$$\mathcal{D}_c^i = K_{i_{Pub}}[h(i, S_{s_c}(q)); \mathcal{D}_c^{i-1}] \tag{7}$$

At decryption time, the dolls are decrypted in reverse order, the i^{th} doll containing, when decrypted, information for the i^{th} trustee and the $(i-1)^{th}$ doll. Only the i^{th} trustee can decrypt the i^{th} doll.

Both dolls are printed at the bottom of both layers, as is q. If $L_b(q)$ is taken by the voter, $\mathcal{D}_t^N$ is decrypted by the Trustees, and information obtained to compute $W_t(q)$ so that $B(q,i,j)$ may be computed for even $i+j$.

Step 5: *The voter checks that the two superimposed layers provide a visual representation of her vote. She checks that there are three numbers also printed at the bottom of both layers, and that the numbers are the same on both layers. She chooses a layer to take away, and communicates it to the Polling Station.*

4.4 Other numbers for commitment checks

After the voter chooses a layer, additional values are printed that enable checking that the layer was correctly generated, and that prevent forgery of a receipt by the voter. Hence, for example, Interested Third Parties can check that the random numbers in the chosen layer were correctly generated.

Step 6: *The Polling Station now prints, only on the chosen layer, (a) the digital signature of q using the public key for the chosen layer and (b) the digital signature of the entire document using the public key for the chosen layer*

More specifically, if $L_c(q)$ is chosen, it prints

$$S_{s_c}(q)$$

and

$$S_{o_c}(L_b(q), q, \mathcal{D}_t^N, \mathcal{D}_b^N, S_{s_c}(q))$$

where c represents t or b.

4.5 Summary

The voter's receipt consists of two layers, the top one reads as follows:

$L_t(q)$

q

$D_t^N(q)$

$D_b^N(q)$

The bottom one reads:

$L_b(q)$

q

$D_t^N(q)$

$D_b^N(q)$

In addition, the chosen layer, c, has the following:

$S_{s_c}(q)$

$S_{o_c}(L_b(q), q, \mathcal{D}_t^N, \mathcal{D}_b^N, S_{s_c}(q))$

5 Election Validity Check Prior to Counting

Step 7:*An Interested Third Party or the voter herself can check that the receipt was correctly generated, as follows.*

Check 1:

The public key of the pair s_c confirms that $S_{s_c}(q)$ is the signature of q.

Check 2:

The random numbers in the chosen layer were generated as specified by equation (1):

$W_c(q) = \sum_i^N h'(h(i, S_{s_c}(q))$

Check 3:

The doll corresponding to the chosen layer was generated as specified by equations (6) and (7)

$$\mathcal{D}_c^1 = K_{1_{Pub}}(h(1, S_{s_c}(q))$$

and

$$\mathcal{D}_c^i = K_{i_{pub}}(h(i, S_{s_c}(q), \mathcal{D}_c^{i-1}))$$

Check 4:

The public key of the pair o_c confirms that $S_{o_c}(L_b(q), q, \mathcal{D}_t^N, \mathcal{D}_b^N, S_{s_c}(q))$ is the signature of $L_b(q), q, \mathcal{D}_t^N, \mathcal{D}_b^N, S_{s_c}(q)$.

These checks are the only way to detect Polling Station cheating, and are hence not "optional". A large enough fraction of receipts must pass these checks for confidence in the election results.

5.1 Aside: Cheating by Polling Station caught with probability half for each changed vote

To cheat successfully, the Polling Station would have to pass all four checks above. In particular, it would have to have generated, and communicated, correctly the random values on the layer chosen by the voter.

Suppose it does generate and communicate correctly the random values on *both* layers. Then, because the two layers together must represent the correct vote, it cannot cheat on the pixels that were not randomly generated. Hence, to cheat, it would have to generate correctly only the random values on one layer and hope the voter takes that one. It can do this with probability only $\frac{1}{2}$ for each incorrect vote if the voter's choices of layer are truly identically distributed. If the Polling Station changes n votes, its probability of successfully cheating would be $(\frac{1}{2})^n$. To create a change in the result of an election, one may assume that n is large enough to make this probability negligible.

If it could predict voter choices, however, the Polling Station could cheat very successfully as follows. It would generate correctly $W(q)$, and then a value of $R(q)$, say Complement Layer, for the vote it chooses, say Fake Vote, so that Fake Vote $= W(q) \oplus$ Complement Layer. It would then generate corresponding $L_t(q)$ and $L_b(q)$. It would guess a layer that the voter would choose, say $L_b(q)$. This layer would contain random numbers correctly generated ($W_b(q)$), which would check correctly. The Polling Station would print $L_b(q)$ and Fake Layer such that $L_b(q) \oplus$ Fake Layer $= B(q)$.

6 Displaying receipts

Step 8: *Receipts are displayed in a publicly accessible place where those with receipts (voters or Interested Third Parties) can check that their receipts (and hence votes) have been correctly retained.*

This step is not optional, and a large enough fraction of receipts must be checked for confidence in election results.

7 Counting

Step 9: *The values of q are stripped, and the collection of votes is passed on to the first trustee*

For a single vote, T_0 is the input to the first trustee, and this is the voter's chosen layer (receipt). Also passed on is the doll for the other layer, so that, together, the trustees may decrypt the vote. Thus the first trustee gets:

$T_0 = L_c$

$\mathcal{D}_{c'}^{N}$

where c' is the complement of the chosen layer.

The random values on the other layers need to be generated to recreate the ballot image. They are generated in parts by each trustee, and added on to the chosen layer sequentially. After the last trustee adds on his part, ballot images are obtained. These may now be counted, in public. Each trustee shuffles his output images, so the original order is not retained and voting is anonymous, with the anonymity being as strong as the trustees' shuffles.

T_i is the output of the i^{th} trustee, and the input to the $(i+1)^{th}$ one. The i^{th} trustee computes T_i by decrypting the doll passed on by the previous trustee. The decryption has two parts. The one part the trustee hashes. The other part forms the next trustee's doll. The following three steps are done by each trustee in sequence.

Step 10: *Doll decryption.* (Compare the equation below with equation (7)).

$K_{i_{Priv}}[\mathcal{D}_{c'}^{N-i}] = (contribution_i, \mathcal{D}_t^{N-(i-1)})$

Step 11: *Add random contribution*

The next step may be compared to equation (1), and $h'(contribution_i)$ seen to be the i^{th} trustee's contribution to the decryption key of the printed encrypted receipt.

$$T_i = T_{i-1} \oplus h'(contribution_i) \tag{8}$$

Step 12: *Shuffle. Retain the shuffle for audit. Pass on shuffled values to Public from where the next trustee obtains them.*

Finally, $W_{c'}$ is reconstructed by every trustee's contributions

$$W_{c'} = \sum_{i=1}^{N} h'(contribution_i)$$

and:

$T_N = B$

Step 13: *The B are counted by Public.*

8 Audit and Certification

Step 14: *An audit of trustee decryption*

The only way to determine that the trustees have not cheated is to check that T_i was correctly constructed from T_{i-1}. For each trustee, this is done as follows:

For half of the images T_i, chosen at random, ask trustee i to provide $contribution_i$ and the correct corresponding image T_{i-1} (they are shuffled). Check that the value of $contribution_i$ is correct wrt equation (7):

$\mathcal{D}_t^i = K_{i_{Pub}}[contribution_i, D_t^{i-1}]$

and that the output T_i was appropriately computed from T_{i-1}, according to equation(8):

$T_i = T_{i-1} \oplus h'(contribution_i)$

The other images are chosen for the audit of the next trustee. Only one audit of the entire election is performed. Each vote a trustee cheats on is detected with probability $\frac{1}{2}$. If the trustee cheats on n votes, the probability that he is not detected is $(\frac{1}{2})^n$.

9 Acknowledgements

Rahul Simha and David himself greatly helped in my understanding of the ideas described in this document.

References

[1] Chaum, David, “Secret Ballot Receipts and Transparent Integrity - Better and less-costly electronic voting at polling places”, http://www.vreceipt.com/article.pdf.

A Notation

K_{pub}: The public key of key pair K

K_{priv}: The private key of key pair K

K_i: key pair for the i^{th} trustee

N: number of trustees

c: one of top or bottom layers

c': the layer other than layer c

o_t: Polling Station key pair for signing the entire receipt, top layer

o_b: Polling Station key pair for signing the entire receipt, bottom layer

s_t: Polling Station key pair for generating W_t

s_b: Polling Station key pair for generating W_b

q: ballot serial number

$S_K(x)$: digital signature of x using public key pair K, or encryption of a specified digest of x using K_{priv}

$B(q)$: the filled-in ballot, binary image, with serial number q

$W(q)$: randomly generated image for serial number q

$R(q)$: complement image for serial number q

$L_t(q)$: top layer of receipt with serial number q

$L_b(q)$: bottom layer of receipt with serial number q

$W_t(q)$: the random numbers in the top layer of receipt q

$W_b(q)$: the random numbers in the bottom layer of receipt q

$\lceil x \rceil$: ceiling(x)

$I(q,i,j)$: the $(i,j)^{th}$ pixel in image $I(q)$

h, h': one-way functions

i: trustee number or row number in image

j: column number in image

n: half the width of the image

$\mathcal{D}_t^N$: encrypted information to generate $W_t(q)$

$\mathcal{D}_b^N$: encrypted information to generate $W_b(q)$

T_i: a generic image output of i^{th} trustee

T_0: a generic input to first trustee

$contribution_i$: value such that $T_i = T_{i-1} \oplus h'(contribution_i)$

B Pseudo-code

A. Constants for election
image width - $2n$
image height - m
number of trustees - N
key pair for the i^{th} trustee: $K_i = (K_{i_{pub}}, K_{i_{priv}})$, $i = 1, 2, ..N$

B. Constants for Polling Station:
Polling Station key pair for signing the entire receipt, top layer; $o_t := (o_{t_{pub}}, o_{t_{priv}})$
Polling Station key pair for signing the entire receipt, bottom layer; $o_b := (o_{b_{pub}}, o_{b_{priv}})$
Polling Station key pair for generating W_t; $s_t := (s_{t_{pub}}, s_{t_{priv}})$
Polling Station key pair for generating W_b; $s_b := (s_{b_{pub}}, s_{b_{priv}})$

C. Primitives:
Generate public/private key pairs (K_{pub}, K_{priv})
Corresponding public key encryption, $E(k, x)$ - encryption of x with key k
Digital signature of x using a given public/private key pair, $K := (K_{pub}, K_{priv})$; $S_K(x)$
Checking a digital signature of x given a public key; $Check\_S(string, x, K_{pub})$
one-way functions h and h'

Election begins

I. At each polling station
For each vote do 1-7

1. Input binary image B, serial number q.

2. Generate 2 random number sequences $W_c(q) := \sum_i^N h'(h(i, S_{s_c}(q))$ of size mn each.

3. Generate the two layers, binary images L_t and L_b.

```
For i going from 1 to m
  For j going from 1 to $2n$
    If $i + j$ even{
      $L_t(q, i, j) := W_t(q, (i - 1) \times n + \lceil \frac{j}{2} \rceil)$
      $L_b(q, i, j) := W_t(q, (i - 1) \times n + \lceil \frac{j}{2} \rceil) \oplus B(q, i, j)$
} End If $i + j$ even
If $i + j$ odd {
$L_t(q, i, j) := W_b(q, (i - 1) \times n + \lceil \frac{j}{2} \rceil) \oplus B(q, i, j)$
$L_b(q, i, j) := W_b(q, (i - 1) \times n + \lceil \frac{j}{2} \rceil)$
} End If $i + j$ odd
End For i and For j

4. Generate dolls for both layers, $\mathcal{D}_t^N$ and $\mathcal{D}_b^N$
For c = top and c=bottom
a. $\mathcal{D}_c^0 := \mathit{empty\_doll}$
b. for i=1 to N
$\mathcal{D}_c^i := E(K_{i_{Pub}}, h(i, S_{s_c}(q)); \mathcal{D}_c^{i-1})$
End For i
End For c

5. Print both layers
a. Top Layer:
$L_t$
$q$
$\mathcal{D}_t^N$
$\mathcal{D}_b^N$
b. Bottom Layer:
$L_b$
$q$
$\mathcal{D}_t^N$
$\mathcal{D}_b^N$

6. Voter chooses layer $c$

7. Print on layer $c$:
$String1 = S_{s_c}(q)$
$String2 = S_{o_c}(L_b(q), q, \mathcal{D}_t^N, \mathcal{D}_b^N, S_{s_c}(q))$

End For each vote

II. Checks:


1. $Check\_S(String1, q, s_{c_{pub}})$
```

```
2a. If c = top
    For i going from 1 to m
        For j going from 1 to 2$n$
            If $i+j$ even
                check if $L_t(q,i,j)? = W_{check}(q,(i-1)\times n+\lceil\frac{j}{2}\rceil)$
                where $W_{check}(q) := \sum_i^N h'(h(i,String1))$
            End $i+j$ even; For i; For j
2b. If c = bottom
    For i going from 1 to m
        For j going from 1 to 2$n$
            If $i+j$ odd
                check if $L_b(q,i,j)? = W_{check}(q,(i-1)\times n+\lceil\frac{j}{2}\rceil)$
                where $W_{check}(q) = \sum_i^N h'(h(i,String1))$
            End $i+j$ even; For i; For j
```

```
3a. $Doll[0] := empty\_doll;$
3b. For i=1 to N
    $Doll[i] := E(K_{i_{pub}},(h(i,string1);doll[i-1]))$
    End For i
3c. If c=top, Check if $Doll[N]? = \mathcal{D}_t^N$
    Else Check if $Doll[N]? = \mathcal{D}_b^N$
```

```
4. $Check\_S(String2, Entire_reecipt, o_{c_{pub}})$
```

III. Counting

```
1. Strip everything on each vote except $L_c$ and $\mathcal{D}_c^N$

2. For all receipts
    $Ballot[receipt,0] := L_c;$
    $Doll[receipt,N] := \mathcal{D}_c^N;$
   End all receipts;

3. For all trustees
    For all receipts
        $(info, Doll[receipt,i-1]) := E(K_{i_{priv}}, Doll[receipt,i]);$
```

```
$Ballot[receipt, i-1] = Ballot[receipt, i] \oplus h'(info)$
End all receipts;
Shuffle receipts; keep copy of shuffle;
End all trustees
```

4. Count Ballot[receipt, N];

IV. Audit

1. Half_set := random selection of half of all receipts

```
2. For all trustees
For all receipts in Half_set
Check if $Ballot[receipt, i-1]? = Ballot[receipt, i] \oplus h'(contrib(receipt))$
Half_set = Complement(Half_set);
End for all receipts
End for all trustees
```