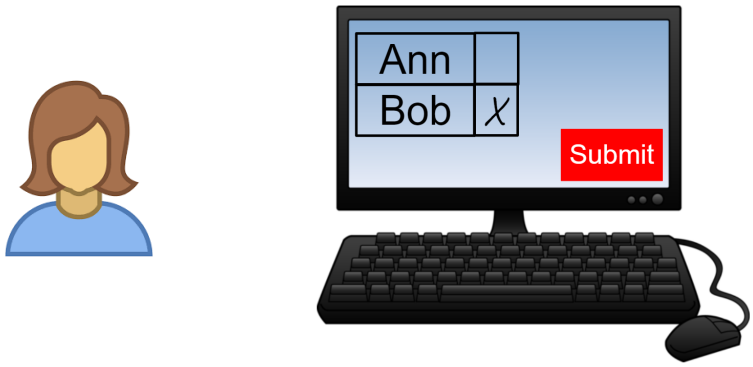
Verification in the VMV System

The VMV Team, University of Surrey
https://vmv.surrey.ac.uk.

VMV (*Verify My Vote*) adds vote verification to a voting system. This allows a voter to confirm that the vote they cast is correctly stored by the system, ensuring that it will be included in the overall count. All votes are published anonymously, meaning that the tally for the election can be independently checked.

Voter view

The voter casts her vote in the normal way: by selecting her choice and submitting it into the system.

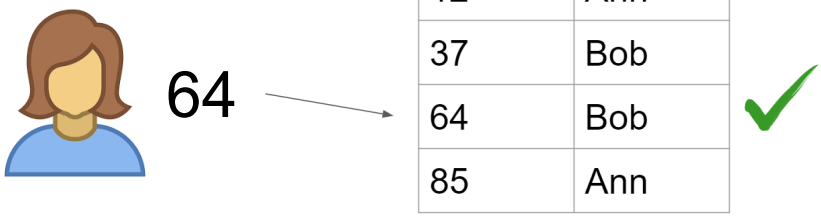


At the end of the election, all of the votes are published, with a unique tracker number against each one.

1	Ann
12	Ann
37	Bob
64	Bob
85	Ann

Each voter privately receives their unique tracker number from VMV.

The voter can check that the vote recorded against that tracker number matches the vote that she cast.



1	Ann
12	Ann
37	Bob
64	Bob
85	Ann

The result of the election is reported as 3 votes for Ann, and 2 votes for Bob. This result can be independently confirmed from the published votes.

Behind the Scenes

The system is designed to safeguard the secrecy of the ballot while ensuring the integrity of the election. It achieves this through the use of cryptography. The technical documentation provides the precise technical details.

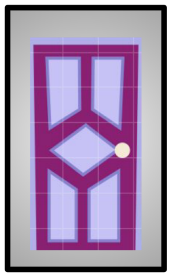
Here we will use analogies to provide an explanation of how the system works.

The system relies on two elements: (1) tracker commitments, and (2) voting envelopes

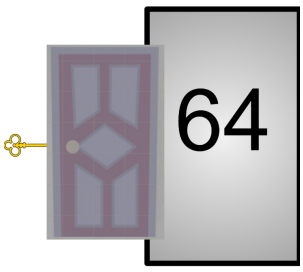
Tracker commitments

Each voter has a unique private key that is not known by anyone else:

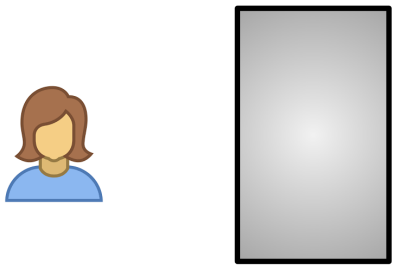
This allows the VMV system to assign a tracker number to each voter but to keep that value secret: by putting it inside a box that can only be opened with the private key. The locked box looks like this:



Only a voter with the private key will be able to open the box to reveal the tracker number:

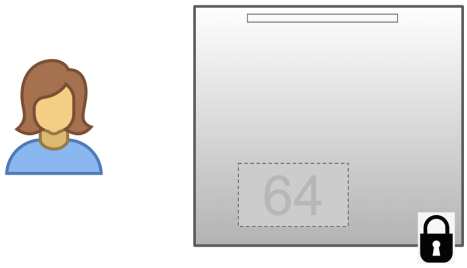


Before the beginning of the election, the door is removed from the box, so that the box without the door is completely sealed. This is given to the voter at the beginning of the election, providing a commitment to the tracker number contained in the box.



Voting envelopes

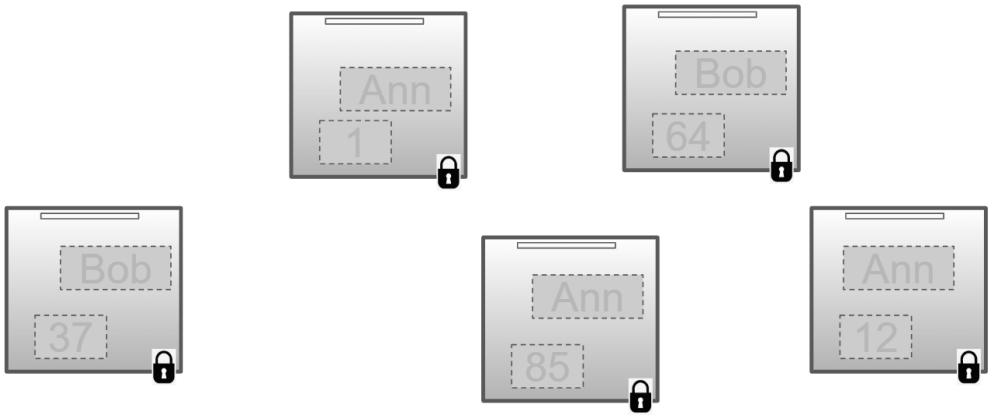
VMV creates a voting envelope for each voter. A voting envelope contains the tracker number assigned to the voter (the same tracker number as in the commitment box), and a slot for a vote to be inserted. The voting envelope can only be opened by the election authorities (with the election key).



Running the election

The voter casts her vote by putting it inside her voting envelope to join the tracker number already in there.

At the end of polling, all of the voting envelopes are collected together and shuffled so that no envelope can be associated with the voter who submitted it.

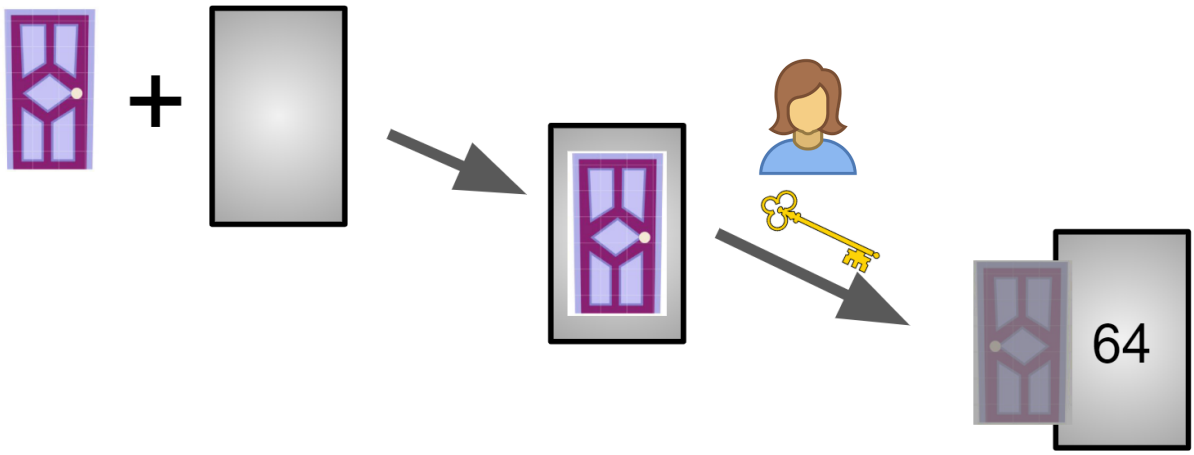


The voting envelopes are then opened by the election authorities. All of the votes are published together with their tracker numbers.

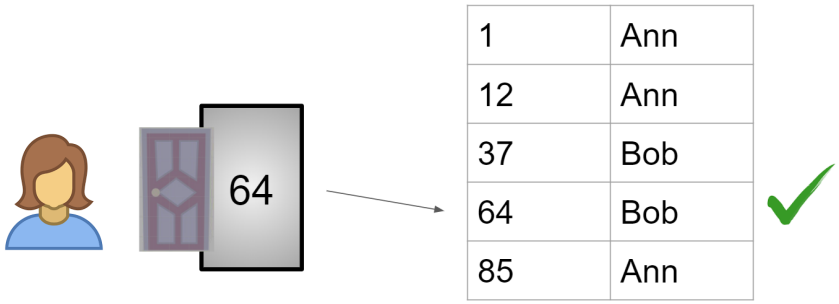
1	Ann
12	Ann
37	Bob
64	Bob
85	Ann

Checking the votes

After all the votes have been published, voters will want to check their votes. VMV sends each voter the door that goes with their tracker commitment box. The voter combines the door and the box, and unlocks it to obtain the tracker number:



She can then check this tracker number on the list of published votes, and confirm that the vote recorded matches the vote that she cast:



1	Ann
12	Ann
37	Bob
64	Bob
85	Ann

Technical Details

The explanation above provides an analogy of what is going on within VMV. The technical details of the system are provided in the Documentation area on the VMV website https://vmv.surrey.ac.uk.

Image Credits

Door image courtesy of www.clipart.email
Person icon courtesy of https://icons8.com
Golden key courtesy of http://www.clker.com
Computer image courtesy of http://clipart-library.com