Electronic voting

Subhashis Banerjee, Subodh Sharma

Computer Science and Engineering
IIT Delhi

August 2020

Voting system: broad objectives

- **Manual identity and eligibility verification** by a polling officer.
- **Offline** electronic voting **with** support for Voter Verified Paper Audit Trails (VVPAT).
- **End of polling upload** of all electronic records to a central server and **electronic counting**.
- **Verifiable** and **publicly auditable**.
- **Zero trust**: no requirement of *trust* on any authority or custody chain.

Verifiability: requirements

For both electronic and VVPAT:

Correctness guarantees (individual):

Cast as intended: Registered correctly in the EVM.

Recorded as cast: Recorded correctly in the tally.

Counted as recorded: Tally is correct.

Correctness guarantees (universal):

No spurious injection: Only votes approved by the PO in the tally.

No spurious deletion: All the cast votes are in the tally.

[Note: Manual paper-based voting can *only* guarantee *cast-as-intended*. *Counted-as-recorded* is futile without *recorded-as-cast*.]

Verifiability: requirements

Software independence:

An undetected change or error in software/hardware should not cause an undetectable change or error in an election outcome [Rivest, 2008; also see Rivest, 2001a, Rivest, 2001b].

Dispute resolution:

Clear determination of any challenge in favour of either the challenger or the election authority.

Zero trust:

No reliance on custody chain.

[Note: The two latter guarantees are not possible in manual paper-based voting.]

Verifiability: requirements

VVPAT:

- A voter should have full agency to cancel a cast vote if not satisfied.
- The process to cancel must be simple and should not require the voter to interact with anybody.
- There should be provable guarantee that all VVPAT slips that are counted in the tally are truly voter verified.
- There should be provable guarantee that no voter verified VVPAT slips are missing from the final tally.
- The VVPAT and electronic system should be integrated and not independent of each other.

EVM only DRE solutions

- An **EVM only** solution is not software independent, hence not verifiable.
- In a system as complicated as an EVM
  1. The *number of states* will be an *exponential* function of the configuration and input parameters.
  2. **Intractable** (at least NP Hard) to determine whether it can ever reach a state that may violate democratic principles [Mercuri, 1992]. May even be **undecidable**.
- Testing - in particular with pre-determined test cases (Quality Assurance) - never adequate.
- None of *cast-as-intended*, *recorded-as-cast* and *counted-as-recorded* guarantees possible.
- The Indian VVPAT solution is not truly voter-verified.

Verifiability: requirements

Universal verifiability:

Verifiable by trusted auditors.

Individual verifiability:

Individuals (or representatives) can verify. Publicly auditable.

Secrecy: requirements

Voter secrecy:

Protocol must not leak voter information. However, **trust on hardware unavoidable**.

Coercion/receipt free:

A voter should not be able to prove to anybody who she voted for.

Community privacy:

Large aggregations to avoid community profiling.

Popular solutions

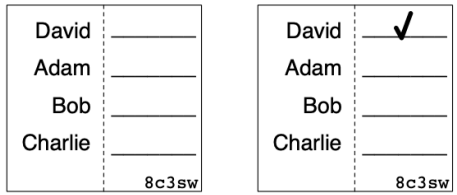
Auditable PrêT à Voter style ballots

PrêT à Voter, Scratch&Vote, Scantegrity

- *Homomorphic* backends (Scratch&Vote).

[Ballots are self-contained and can be publicly audited on the spot]

- *Mixnet* based backends (PrêT à Voter, Scantegrity I and II).



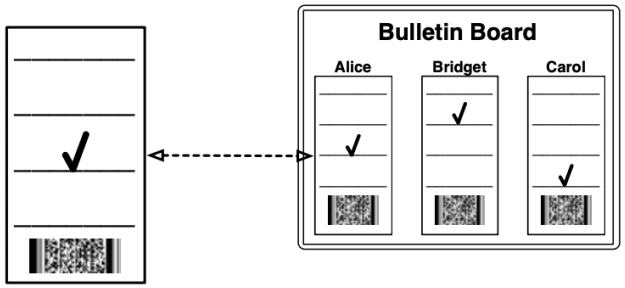
[Ballot audit requires a *cast-or-challenge* audit (later) of the *mixnet*]

- The left part is discarded after polling, the right part is scanned at the EVM and taken home as receipt.

Scratch & Vote: an example of a verifiable voting system

[Adida and Rivest, 2006]

- Receipts are displayed on a public bulletin board.



- Public homomorphic counting.

$$E(m_1) \times E(m_2) \times \ldots \times E(m_n) = E(m_1 + m_2 + \ldots + m_n)$$

- *Zero Knowledge Proof* (ZKP) of decryption of final result.
- Not compatible with VVPAT. The VVPAT system needs to be completely independent.

Paillier encryption (homomorphic): a detour

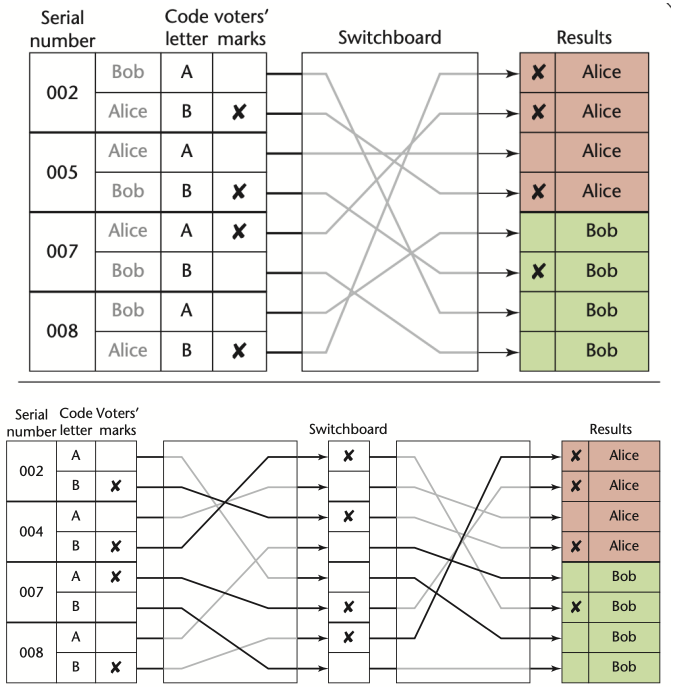
- $\mathsf{Gen}(1^k)$: generate two safe primes p_1 and p_2 . The secret key s_k is $\lambda = \mathsf{lcm}(p_1 - 1, p_2 - 1)$. The public key p_k includes $n = p_1 p_2$ and $g \in \mathbb{Z}_{n^2}$ such that $g = 1 \bmod n$. Often times, $g = n + 1$.
- $\mathsf{Enc}_{p_k}(m; r)$: encrypt a message $m \in \mathbb{Z}_n$ with randomness $r \in \mathbb{Z}_{n^2}$ and public key p_k as $c = g^m r^n \bmod n^2$. We write $c = \mathsf{Enc}_{p_k}(m)$ when the randomness r is not crucial to the explanation.
- $\mathsf{Dec}_{s_k}(c)$: decrypt a ciphertext $c \in \mathbb{Z}_{n^2}$. Consider the function $L(x) = (x - 1)/n$. Decryption is then:

$$\frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$$

[Paillier, 1999]

Scantegrity II: Mixnet based encryption

[Chaum et al., 2008]



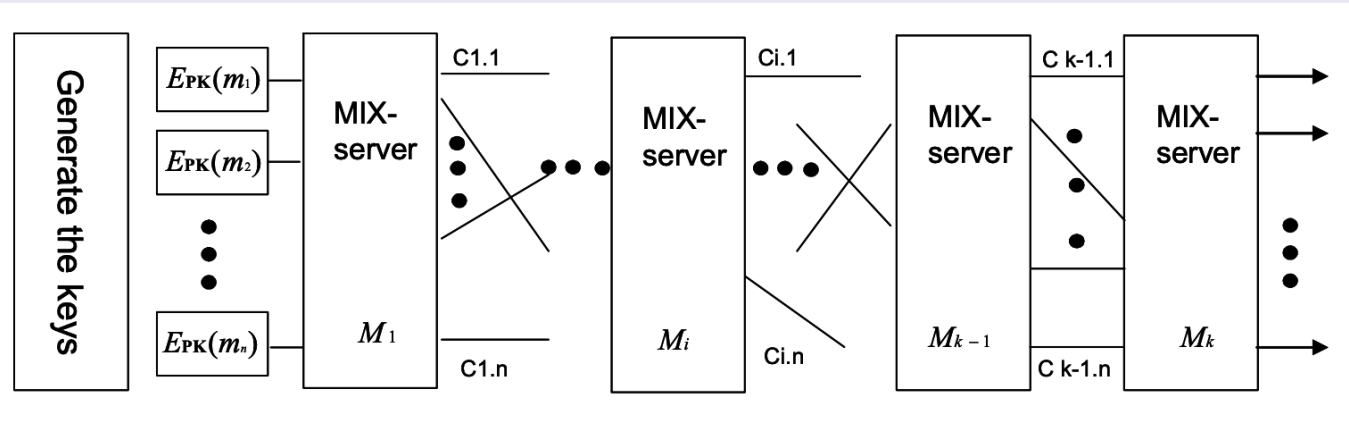
- Voters can verify receipts displayed on a public bulletin board at the input of the *mixnet*. Public counting at the output of the *mixnet*.
- ZKP of the *mixnet* encryption possible.
- Not compatible with VVPAT. The VVPAT system needs to be completely independent.

Difficulties

- Conversion to DRE (no scan) requires EVM to printout the marked ballot for the voter to verify against the original. The voter needs to discard the LHS and retain the RHS of both.
- Homomorphic code in Scratch&Vote too large to fit into the ballot for 20 or more candidates.
- Scantegrity II ballots are not auditable on the spot. Requires a Mixnet audit service.
- Mixnet not (normally) publicly auditable. Requires trusted verifiers/auditors. ZKP possible.

Mixnets: a detour

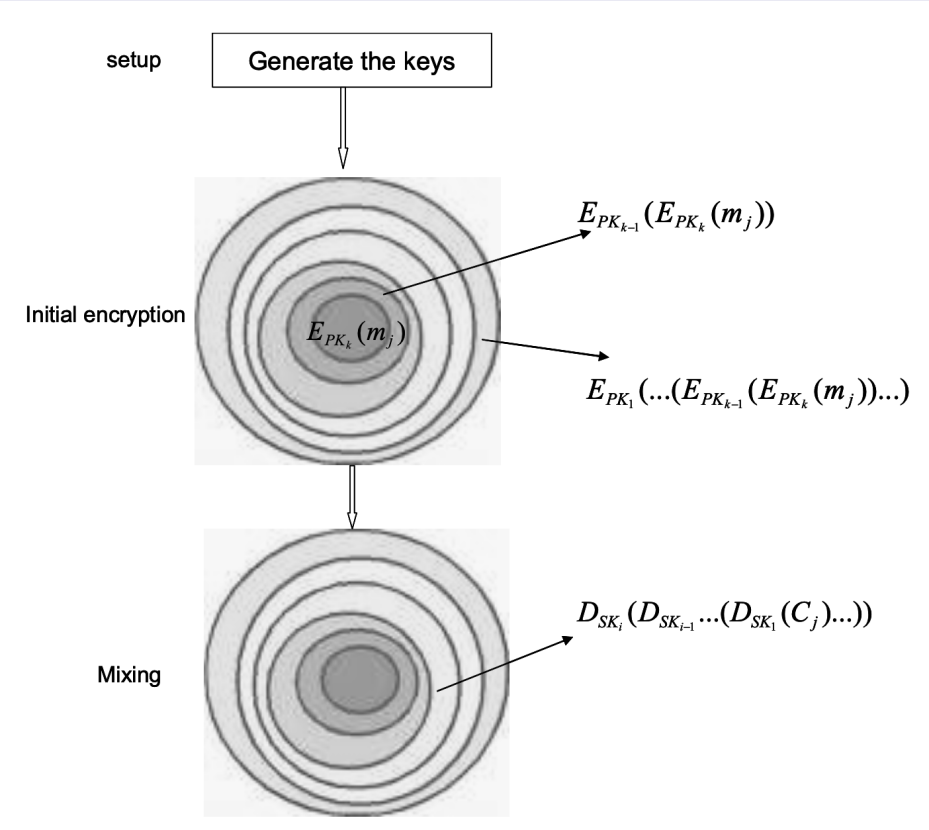
A mixnet



Each mix server permutes the input

Chaumian mixnets

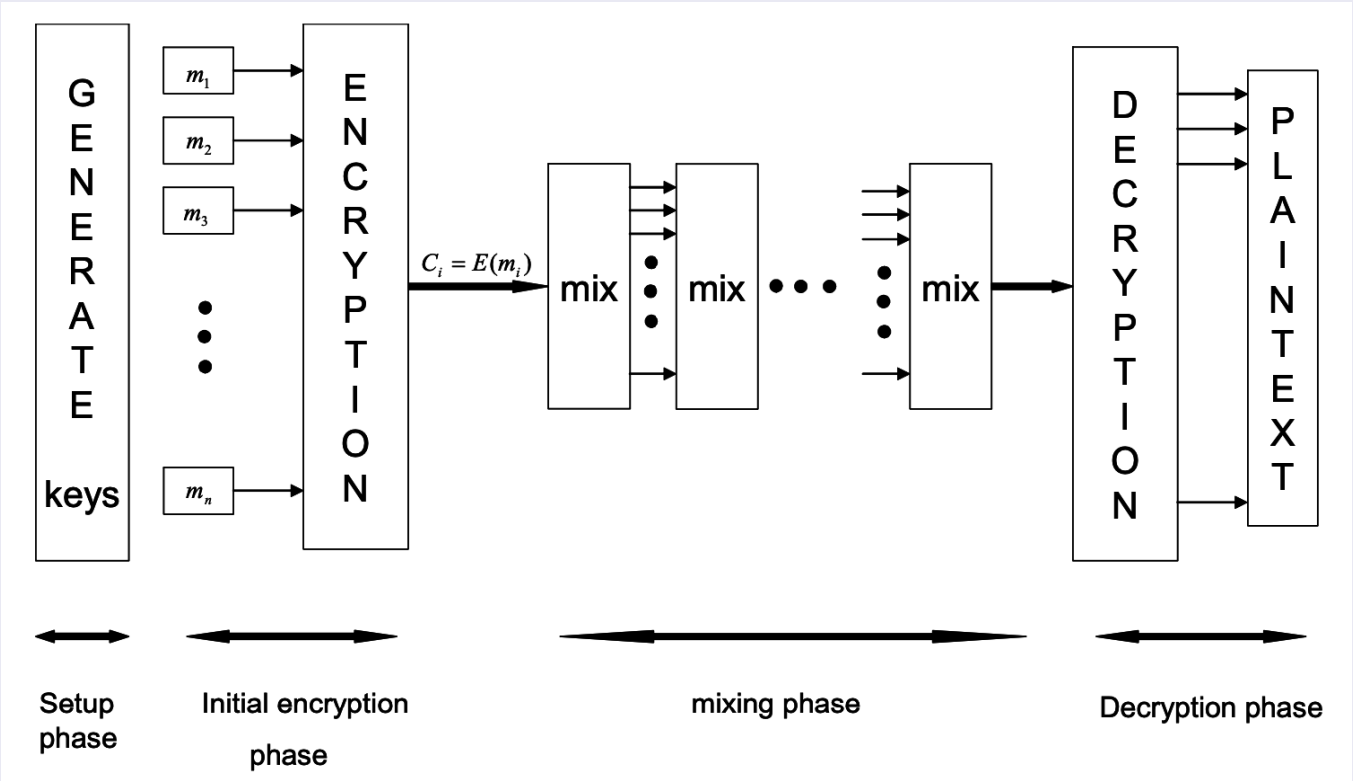
Onion



Also called a decryption mixnet [Chaum, 1981]

Re-encryption mixnets

Re-encryptions



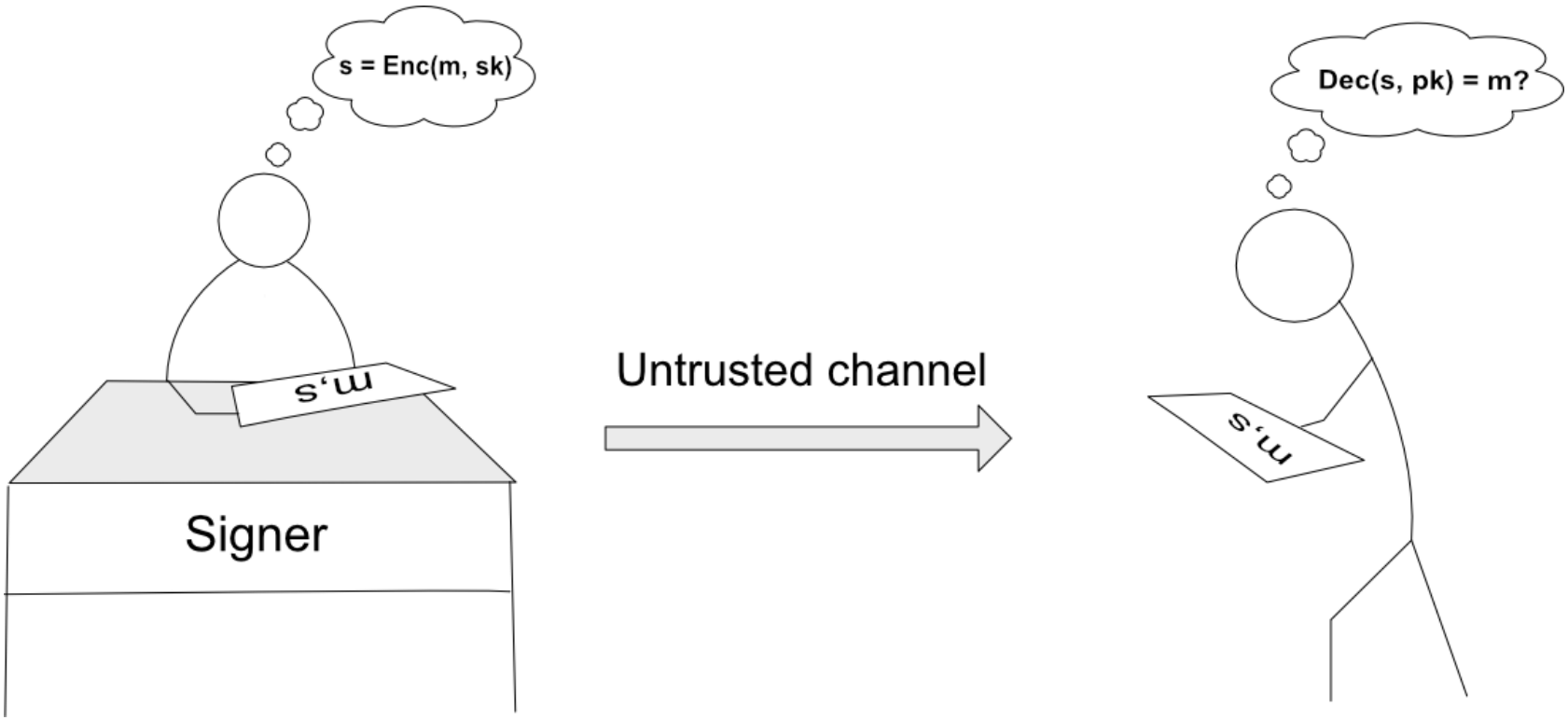
Secret sharing among k parties or multi-party computation

DRE without pre-printed ballots

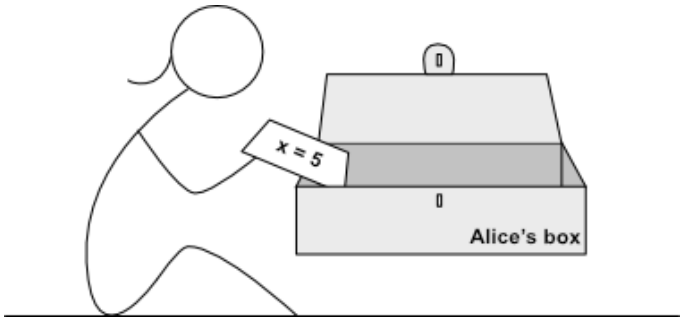
- *Recorded-as-intended* guarantees will require an interactive challenge-response with the voter.
- In Markpledge [Adida and Neff, 2009] - a well known DRE protocol - the voter needs to challenge and match 5 digits strings for the guarantee to establish.
- In Star Vote [Bell et al., 2013] - a scheme deployed and tested in large elections - at least some (almost 50%) voters have to cast false votes and challenge the encryption.

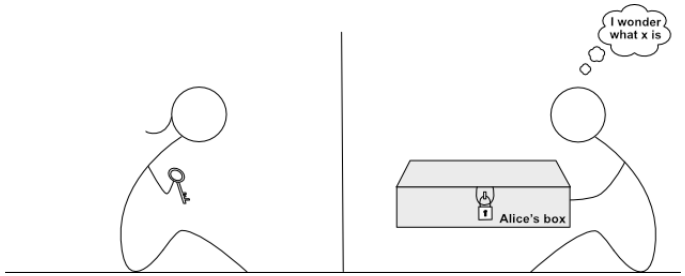
A proposal

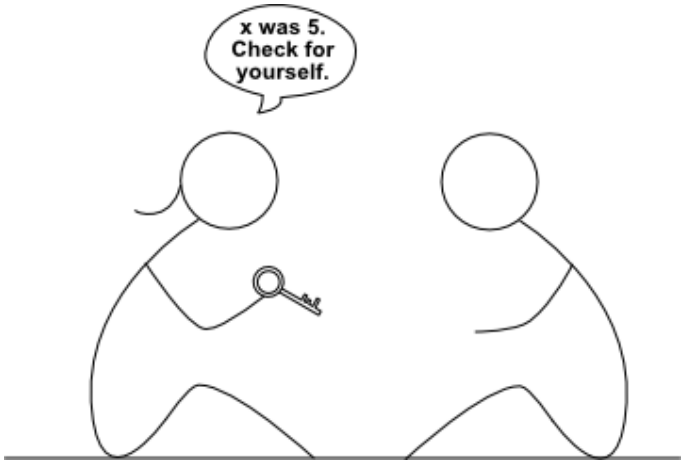
Crypto basics: Digital signatures (Diffie and Hellman 2006)



Crypto basics: Commitment (Brassard, Chaum and Crepeau 1988)







Crypto basics: Modular groups

- The set $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ is the set of all remainders modulo n. $\mathbb{Z}_n$ supports two basic operations, addition and multiplication, in the obvious way. For example, $(11 + 13) = 8 \pmod{16}$ and $(11 \cdot 13) = 15 \pmod{16}$.
- A *group* is a set with an operation which is closed, has an identity, is associative, and every element has an inverse. In addition, a group which is commutative is called *abelian*.
- An abelian group is called *cyclic* if there is a special element, called the *generator*, from which every other element can be obtained. ($G = \langle g \rangle$)
- Every element h of G can be written as $h = g^x$ for some integer x.

Crypto basics: Modular groups

- If $n = p$ is a prime, then for all non-zero $a \in \mathbb{Z}_p$, $ax = 1 \pmod{p}$ has a unique solution and a has a multiplicative inverse.
- If G is a subgroup of $\mathbb{Z}_p^*$ of size q, then q divides $p - 1$.
- We choose large primes p and q such that q divides $p - 1$, G_q is a unique cyclic subgroup of $\mathbb{Z}_p^*$ of order q, and g and h are generators of G_q.
- We assume that g and h are system initialized and publicly known, but the discrete logarithm $\log_g h$ is not known to anybody and is hard to compute.

Crypto basics: Pedersen commitment

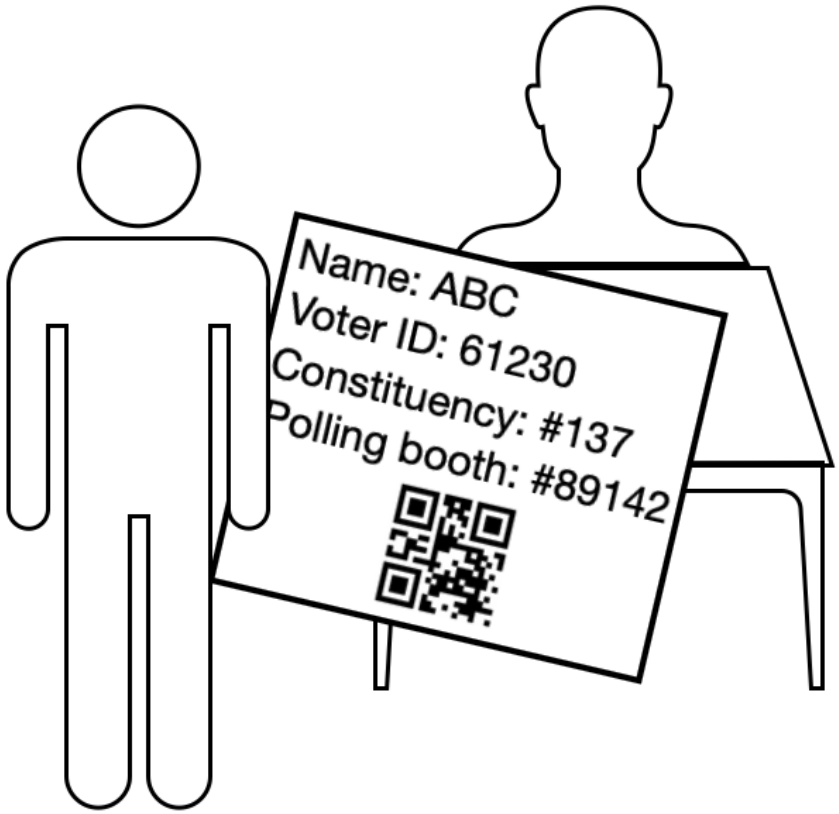
- Given a message $\rho \in \mathbb{Z}_q$ the Pedersen commitment is $C = g^{\rho} h^{r}$, where $r \in \mathbb{Z}_q$ is a secret randomness.
- The Pedersen commitment is *perfectly hiding*.
- The Pedersen commitment is *computationally binding*: $C = g^{\rho} h^{r} = g^{\rho'} h^{r'}$ reveal that $\log_g(h) = (\rho - \rho')/(r' - r) \mod q$.
- The Pedersen commitment is *additively homomorphic*, i.e., if $C_1 = g^{\rho_1} h^{r_1}$ and $C_2 = g^{\rho_2} h^{r_2}$ are commitments of ρ_1 and ρ_2 respectively, then $C_1 * C_2 = g^{\rho_1+\rho_2} h^{r_1+r_2}$ is a commitment of $\rho_1 + \rho_2$.

Crypto basics: ZKP of set membership (Camenisch 2008)

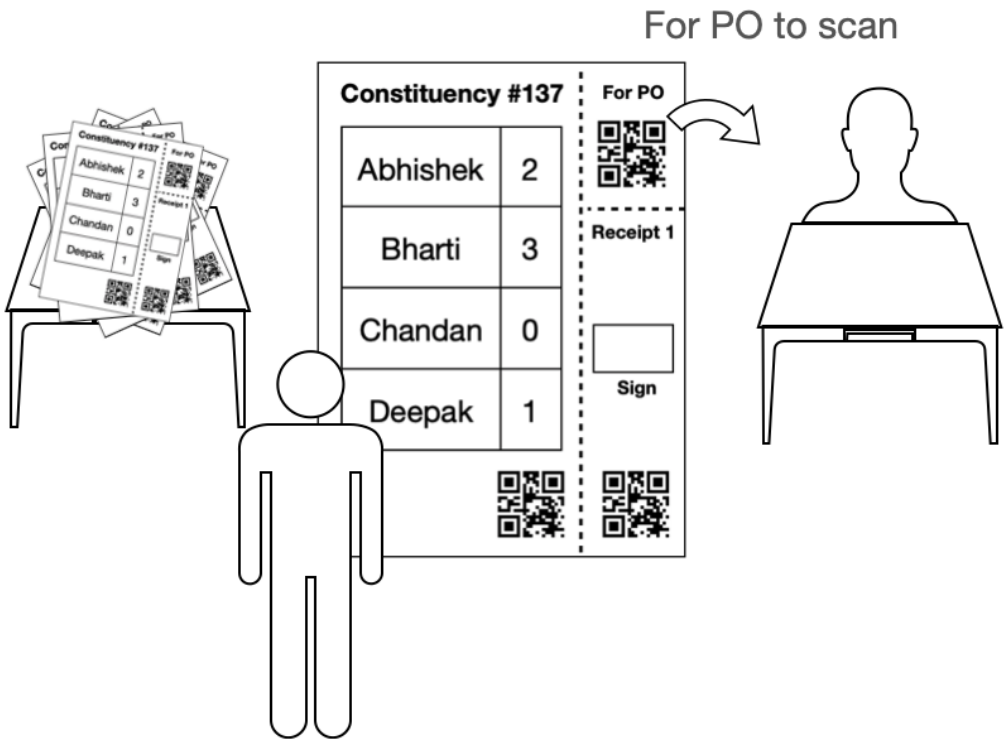
- For an instance of commitment C, a proof of set membership with respect to a publicly known set Φ is a *zero knowledge proof of knowledge* of (ρ, r) such that $C = g^{\rho} h^{r} \wedge \rho \in \Phi$.
- If Φ is stored indexed by C, then the ZKP of set membership is computationally efficient and requires only $O(1)$ sized proofs.

[Camenisch 2008]

Manual offline eligibility and identity verification



Ballot selection

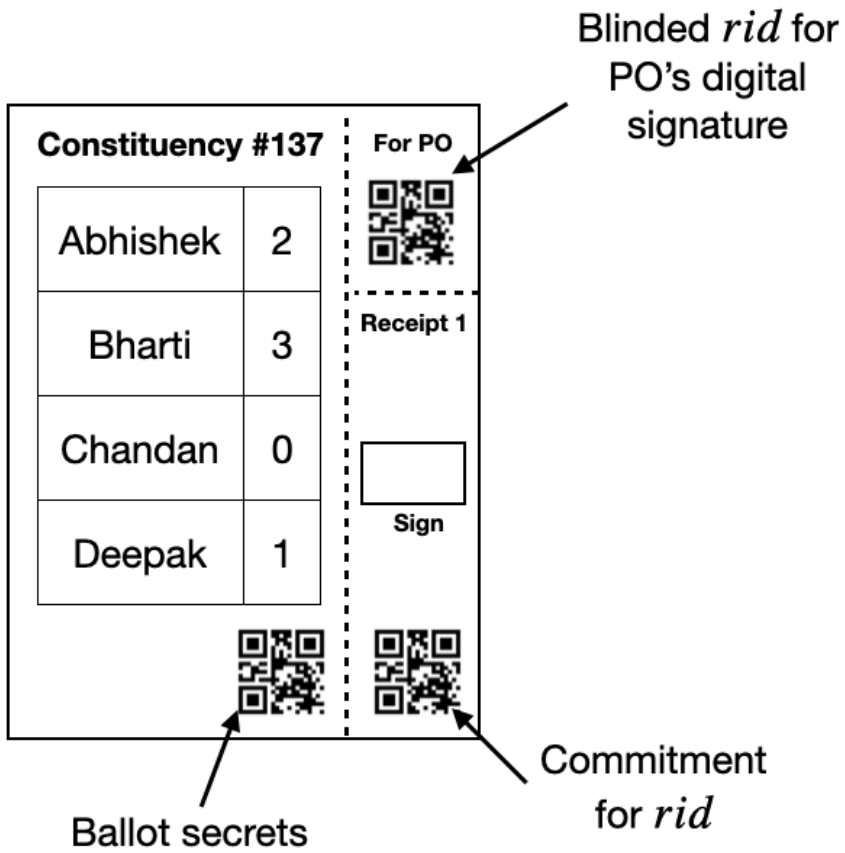


The self contained ballots may be pre-audited by anybody.

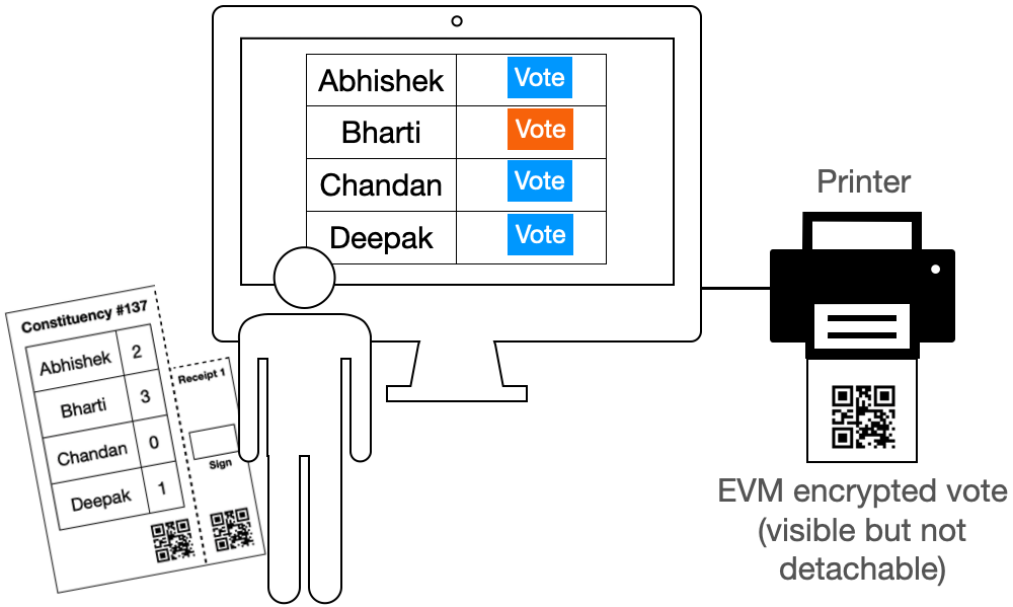
The ballot

1. A random id and the corresponding commitment: $rid_i \in_R \mathbb{Z}_q$, $C_{rid_i} = g^{rid_i} h^{r_{I_i}}$.
2. An obfuscation key and the corresponding commitment: $u_i \in_R \mathbb{Z}_q$, $C_{u_i} = g^{u_i} h^{r_{u_i}}$.
3. The signed the commitments $\sigma_{u_{ik}} = \text{sign}_{p_k}(C_{u_i})$ and $\sigma_{rid_{ik}} = \text{sign}_{p_k}(C_{rid_i})$.
4. **QR1**: Blinded rid_i: b_{rid_i}; **QR2**: $(C_{rid_i}, \sigma_{rid_{ik}})$, $(C_{u_i}, \sigma_{u_{ik}})$; **QR3**: the random secrets (r_{I_i}, r_{u_i}), (rid_i, u_i) and $(u_i \bmod m)$.
5. The random numbers $((u_i \bmod m + v_i) \bmod m)$ (where m is the number of candidates) against each candidate v_i.

Ballot design

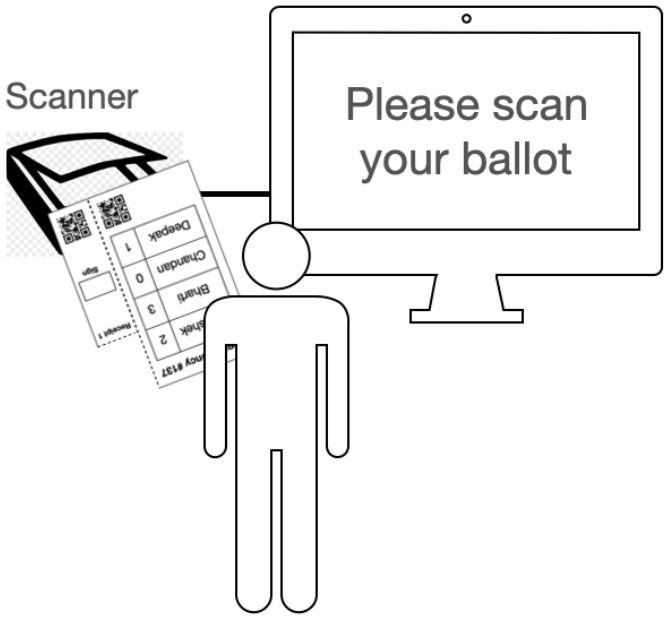


Vote selection at the EVM



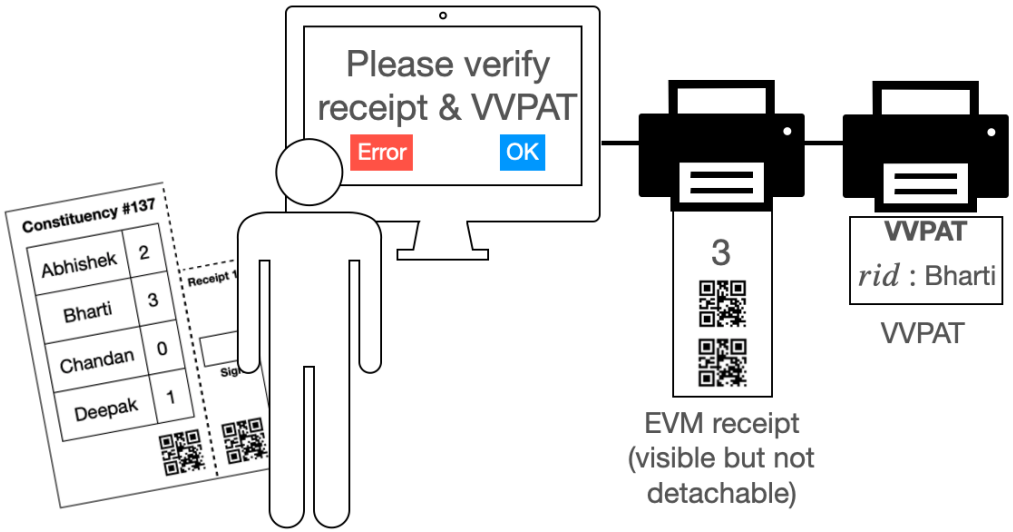
The EVM displays the candidate order for the constituency, the voter presses a button corresponding to her choice.

Ballot scan at the EVM



The EVM reads the two QR codes containing a) a cryptographic commitments of *rid* and u_i and b) ballot encoding secrets.

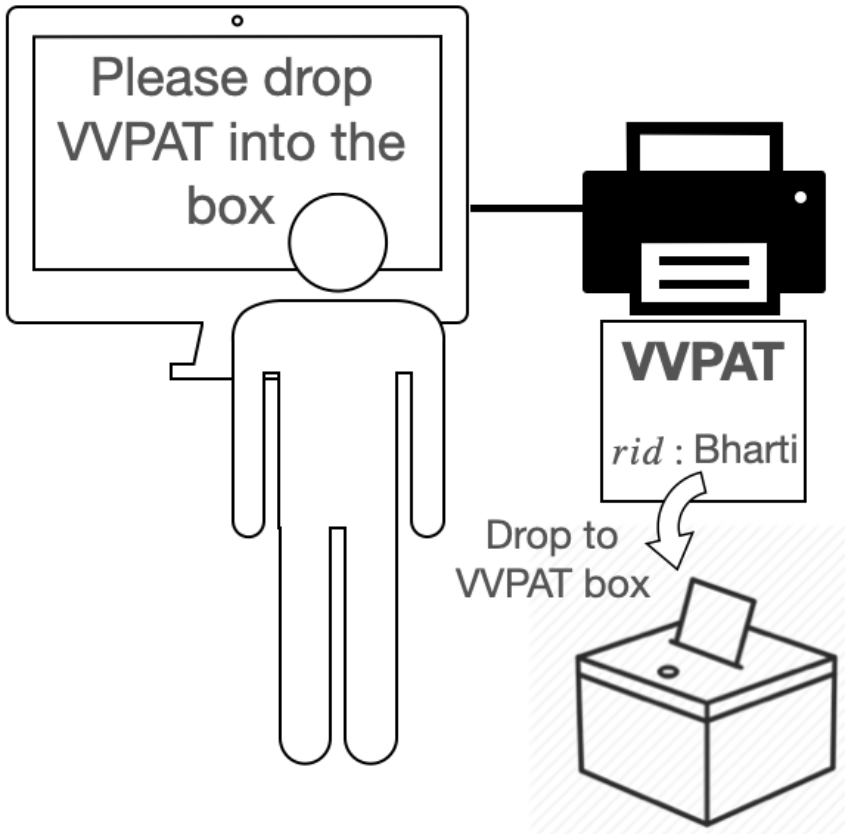
Receipt verification



The voter verifies the number printed on the receipt against her choice on the ballot. These numbers can be encoded in symbols.

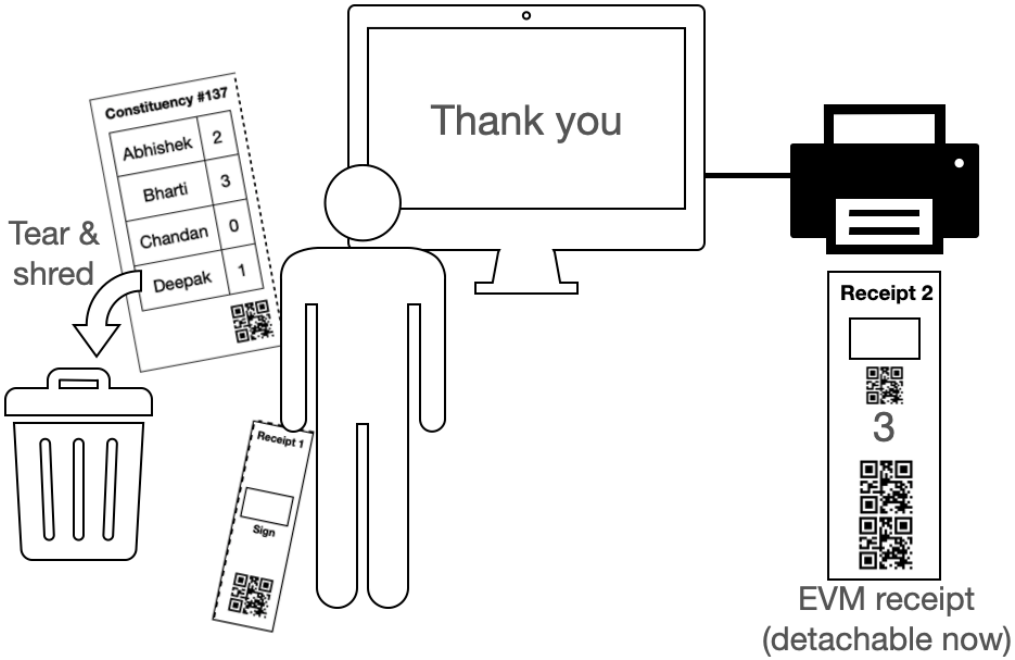
The voter also verifies the VVPAT printout containing her vote in the clear.

VVPAT



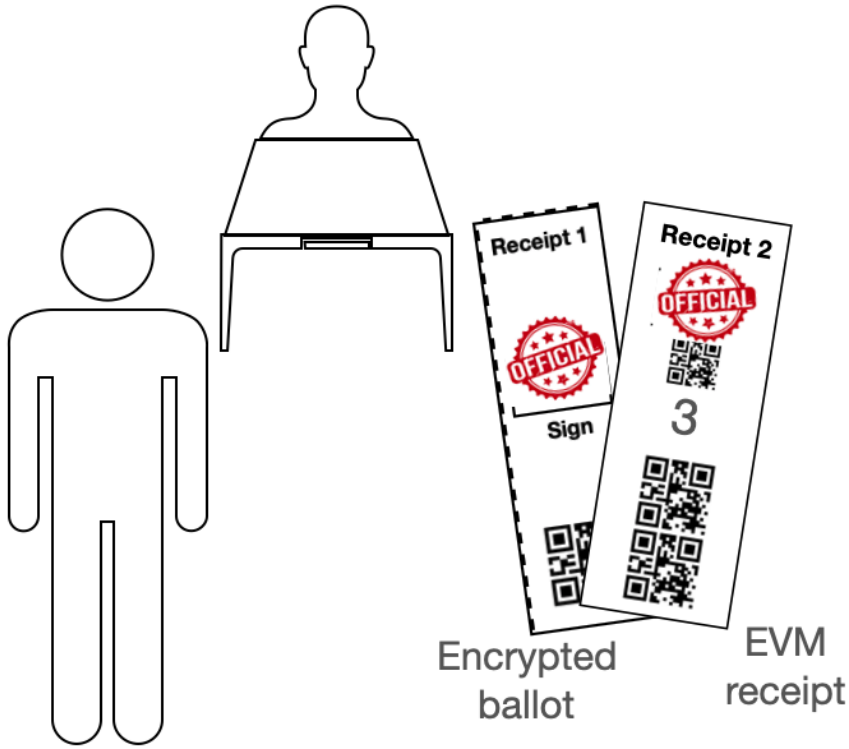
The voter deposits the VVPAT printout in the VVPAT box. Her vote casting is incomplete without this step.

Receipt issue



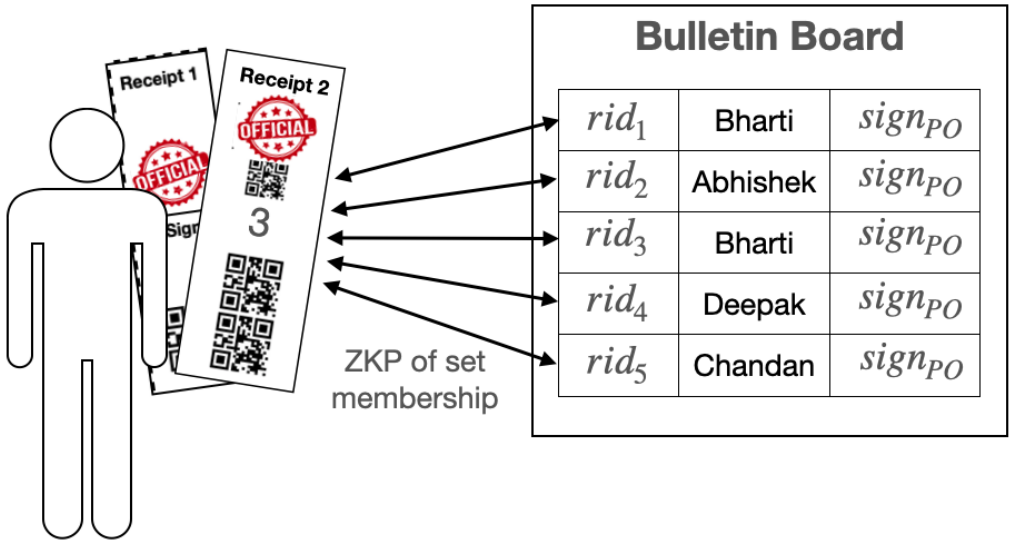
The EVM issues a receipt. The voter discards the part of the ballot containing secrets.

The polling officer certifies casting of vote



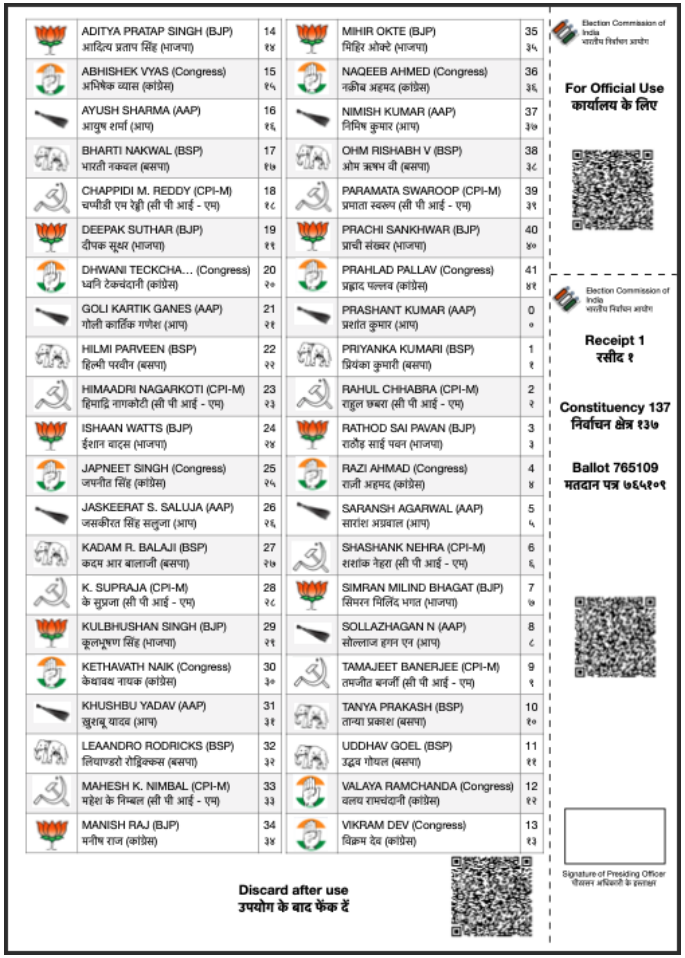
The polling officer stamps the two receipts certifying that vote has been cast according to protocol. Digitally signs and uploads QR codes of all such ballots at the end of polling.

Tally on a public bulletin board



- Public computation of the tally on a bulletin board. Voters can verify using their receipts that their votes are correctly recorded.
- 1–1 correspondence of VVPAT slips and votes recorded on the public bulletin board.

True-size ballot design



ADITYA PRATAP SINGH (BJP) आदित्य प्रताप सिंह (भाजपा)	14 १४	MIHIR OKTE (BJP) मिहिर ओक्टे (भाजपा)	35 ३५
ABHISHEK VYAS (Congress) अभिषेक व्यास (कांग्रेस)	15 १५	NAQEEB AHMED (Congress) नक़ीब अहमद (कांग्रेस)	36 ३६
AYUSH SHARMA (AAP) आयुष शर्मा (आप)	16 १६	NIMISH KUMAR (AAP) निमिष कुमार (आप)	37 ३७
BHARTI NAKWAL (BSP) भारती नकवाल (बसपा)	17 १७	OHM RISHABH V (BSP) ओम ऋषभ वी (बसपा)	38 ३८
CHAPPIDI M. REDDY (CPI-M) चप्पीडी एम रेड्डी (सी पी आई - एम)	18 १८	PARAMATA SWAROOP (CPI-M) प्रमाता स्वरूप (सी पी आई - एम)	39 ३९
DEEPAK SUTHAR (BJP) दीपक सूथर (भाजपा)	19 १९	PRACHI SANKHWAR (BJP) प्राची संखवर (भाजपा)	40 ४०
DHWANI TECKCHA... (Congress) ध्वनि टेकचंदानी (कांग्रेस)	20 २०	PRAHLAD PALLAV (Congress) प्रह्लाद पल्लव (कांग्रेस)	41 ४१
GOLI KARTIK GANES (AAP) गोली कार्तिक गणेश (आप)	21 २१	PRASHANT KUMAR (AAP) प्रशांत कुमार (आप)	0 ०
HILMI PARVEEN (BSP) हिल्मी परवीन (बसपा)	22 २२	PRIYANKA KUMARI (BSP) प्रियंका कुमारी (बसपा)	1 १
HIMAADRI NAGARKOTI (CPI-M) हिमाद्रि नागकोटी (सी पी आई - एम)	23 २३	RAHUL CHHABRA (CPI-M) राहुल छबरा (सी पी आई - एम)	2 २
ISHAAN WATTS (BJP) ईशान वाट्स (भाजपा)	24 २४	RATHOD SAI PAVAN (BJP) राठौड़ साई पवन (भाजपा)	3 ३
JAPNEET SINGH (Congress) जपनीत सिंह (कांग्रेस)	25 २५	RAZI AHMAD (Congress) राज़ी अहमद (कांग्रेस)	4 ४
JASKEERAT S. SALUJA (AAP) जसकीरत सिंह सलुजा (आप)	26 २६	SARANSH AGARWAL (AAP) सारांश अग्रवाल (आप)	5 ५
KADAM R. BALAJI (BSP) कदम आर बालाजी (बसपा)	27 २७	SHASHANK NEHRA (CPI-M) शशांक नेहरा (सी पी आई - एम)	6 ६
K. SUPRAJA (CPI-M) के सुप्रजा (सी पी आई - एम)	28 २८	SIMRAN MILIND BHAGAT (BJP) सिमरन मिलिंद भगत (भाजपा)	7 ७
KULBHUSHAN SINGH (BJP) कुलभूषण सिंह (भाजपा)	29 २९	SOLLAZHAGAN N (AAP) सोल्लाज हगन एन (आप)	8 ८
KETHAVATH NAIK (Congress) केथावथ नायक (कांग्रेस)	30 ३०	TAMAJEET BANERJEE (CPI-M) तमजीत बनर्जी (सी पी आई - एम)	9 ९
KHUSHBU YADAV (AAP) खुशबू यादव (आप)	31 ३१	TANYA PRAKASH (BSP) तान्या प्रकाश (बसपा)	10 १०
LEAANDRO RODRICKS (BSP) लियाण्डरो रोड्रिक्स (बसपा)	32 ३२	UDDHAV GOEL (BSP) उद्धव गोयल (बसपा)	11 ११
MAHESH K. NIMBAL (CPI-M) महेश के निम्बाल (सी पी आई - एम)	33 ३३	VALAYA RAMCHANDA (Congress) वलय रामचंदानी (कांग्रेस)	12 १२
MANISH RAJ (BJP) मनीष राज (कांग्रेस)	34 ३४	VIKRAM DEV (Congress) विक्रम देव (कांग्रेस)	13 १३

Discard after use
उपयोग के बाद फेंक दें

Election Commission of India
भारतीय निर्वाचन आयोग

For Official Use
कार्यालय के लिए

Election Commission of India
भारतीय निर्वाचन आयोग

Receipt 1
रसीद १

Constituency 137
निर्वाचन क्षेत्र १३७

Ballot 765109
मतदान पत्र ७६५१०९

Signature of Presiding Officer
पीठासन अधिकारी के हस्ताक्षर

*For a constituency with 42 candidates.

Protocol: At the EVM

1. Verify ballot tokens and commitments.
2. Sets $\rho_i = rid_i + v_i$, $w_i = u_i + v_i$ and $w_i' = w_i \bmod m$.
3. $C_{v_i} = g^{v_i} h^{r_{v_i}}$, where $r_{v_i} \in \mathbb{Z}_q$ is a secret randomness. $\mu_{v_{ik}} = \text{sign}_{e_k}(C_{v_i})$.
4. EVM $\rightarrow$ voter: $(C_{v_i} \mu_{v_{ik}})$ and $P_i = (w_i, w_i', r_{w_i} = r_{u_i} + r_{v_i})$, a proof that $C_{u_i} * C_{v_i}$ is a commitment of w_i.
5. Voter $\rightarrow$ EVM: Acknowledgement that w_i' is correct.
6. Compute hash $h_i = \mathcal{H}((rid_i, v_i))$ where $\mathcal{H}$ is a publicly known, collision and preimage resistant cryptographic hash function.
7. $s_i = \langle rid_i, u_i, v_i, r_{I_i}, r_{u_i}, r_{v_i} \rangle$
8. $m_i = \langle (C_{rid_i}, \sigma_{rid_{ik}}), (C_{u_i}, \sigma_{u_{ik}}), (C_{v_i}, \mu_{v_{ik}}), (P_i, \mu_{P_{ik}}), (h_i, \mu_{h_{ik}}) \rangle$
9. Store record $\text{enc}_{P_{EA}} \langle s_i, m_i \rangle$ indexed by b_{rid_i}.

Protocol: At the polling booth, after voting is over

1. Polling officer $\rightarrow$ EVM$_k$: The printouts $(b_{rid_i}, ack_i, \sigma_{ack_{ik}})$ for all successful voters for scanning.
2. EVM$_k$: adds $(ack_i, \sigma_{ack_{ik}})$ to the records $\text{enc}_{P_{EA}}\langle s_i, m_i\rangle$ corresponding to b_{rid_i}.
3. N_k is the count of valid votes acknowledged by the polling officer. $\sigma_{N_k} = \text{sign}_{p_k}(N_k)$
4. EVM$_k$: Compute $H_k = \bigoplus_i h_i$ and $\mu_{H_k} = \text{sign}_{e_k}(H_k)$.
5. EVM$_k$ $\rightarrow$ polling officer: (H_k, μ_{H_k}) (printout or in electronic form for the polling officer).
6. The polling officer publishes $(H_k, \mu_{H_k}), (N_k, \sigma_{N_k})$ along with the name of the polling booth and the constituency on a bulletin board $\mathcal{BB}_1$.

Protocol: Collection, for each EVM, after voting is over

1. Carry out a hardware and software integrity check of the EVM and discard if found problematic.
2. Collect each $\langle \text{enc}_{P_{EA}} \langle s_i, m_i \rangle, (ack_i, \sigma_{ack_{ik}}) \rangle$ indexed by b_{rid_i}.
3. Post collection from all EVMs, randomize the records $\langle b_{rid_i}, \text{enc}_{P_{EA}} \langle s_i, m_i \rangle, (ack_i, \sigma_{ack_{ik}}) \rangle$ using a *shuffler*. and upload to the election authority through a secure and private channel.

Protocol: At the election authority

1. Decrypt each $b_{rid_i}, \langle \text{enc}_{P_{EA}} \langle s_i, m_i \rangle, (ack_i, \sigma_{ack_{iM}}) \rangle$. Unblind. Audit each row.
2. Store each record indexed by $C_i = C_{rid_i} * C_{v_i}$ and C_{rid_i}.
3. (optional) Publish each $[C_{rid_i}, w_i = u_i + v_i]$ on a bulletin board $\mathcal{BB}_2$, sorted by C_{rid_i}.
4. Publish rows $[rid_i, v_i, \rho_i = rid_i + v_i, (h_i, \mu_{h_{iM}})]$ on a bulletin board $\mathcal{BB}_3$, sorted by rid_i. The first column of the table is the set Ψ and the third column is the set Φ. Anybody can download and verify the signature on h_i using the public key of the collection authority; also h_i.
5. Demonstrate that $\bigoplus_k H_k = \bigoplus_i h_i$ and $\sum_k N_k = N$, where N is number of rows in $\mathcal{BB}_3$.
6. Tally the votes on $\mathcal{BB}_3$ and publish. Anybody can download and verify.

Protocol: Voter-verified accountability

1. $V_i \rightarrow$ Trusted Verifier: Receipts containing $(C_{rid_i}, \sigma_{rid_{ik}})$, $(C_{u_i}, \sigma_{u_{ik}})$ from ballot; $(C_{v_i}, \mu_{v_{ik}})$, $(P_i, \mu_{P_{ik}})$ where $P_i = (w_i, w_i', r_{w_i})$ from EVM.
2. Trusted Verifier: Check that all signatures match, that $C_{u_i} * C_{v_i} = g^{w_i} h^{r_{w_i}}$ and $w_i' = w_i \mod m$.
3. Trusted Verifier - $\rightarrow$ EA: $\langle C_{rid_i}, C_{v_i} \rangle$.
4. EA $\leftrightarrow$ Trusted Verifier: Provide ZKPs that $C_i = C_{rid_i} * C_{v_i}$ corresponds to a $rid_i + v_i \in \Phi$ and C_{rid_i} corresponds to a row in Ψ.