Masked Ballot Voting for Receipt-Free Online Elections

Roland Wen and Richard Buckland

School of Computer Science and Engineering
The University of New South Wales
Sydney, Australia
{rolandw,richardb}@cse.unsw.edu.au

VOTE-ID 2009

Outline

Receipt-Freeness in Online Elections

- Online elections have great potential but serious concerns remain
- Elections have unique and challenging security requirements
  - Secret ballot prevents bribery and coercion
  - $\Rightarrow$ Voters can lie to 3rd parties
- Receipt-freeness: voters cannot prove how they voted
  - No receipt (evidence) for the vote

Why Is Receipt-Freeness Difficult?

1. Electronic data is easy to copy
   - $\Rightarrow$ Easy to produce electronic evidence for the vote
2. Plausible there could be a powerful adversary who intercepts all Internet communication (eg packet sniffing by ISPs)
   - $\Rightarrow$ Verify evidence

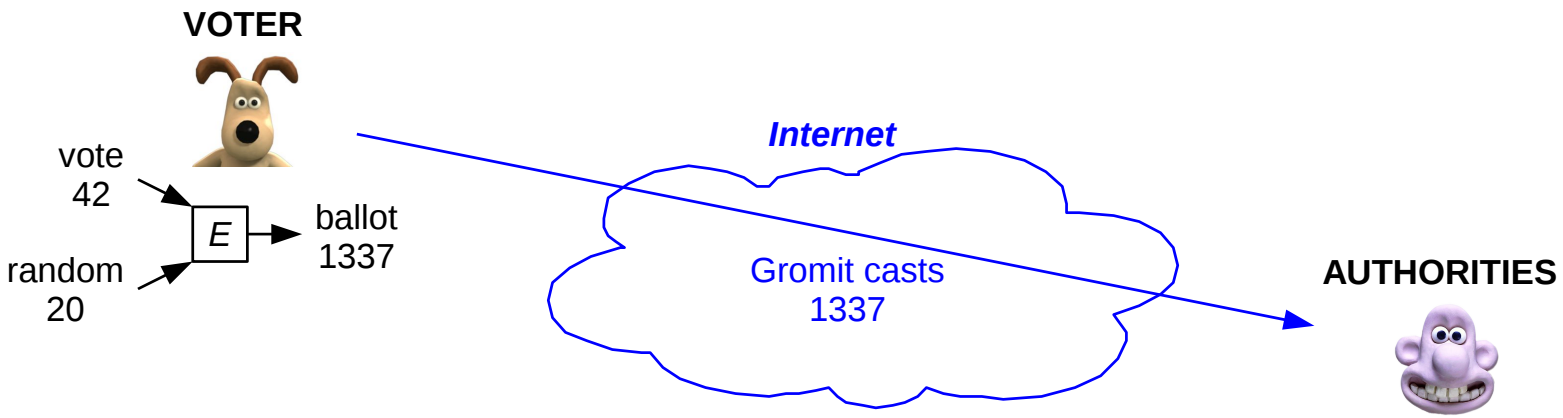
- Need secret information that prevents adversary from verifying evidence
  - $\Rightarrow$ Strong assumptions during the election
  - Hard to realise assumptions in practice

Example: A Flawed Scheme

- Hypothetical voting scheme: voters and authorities only communicate via the Internet

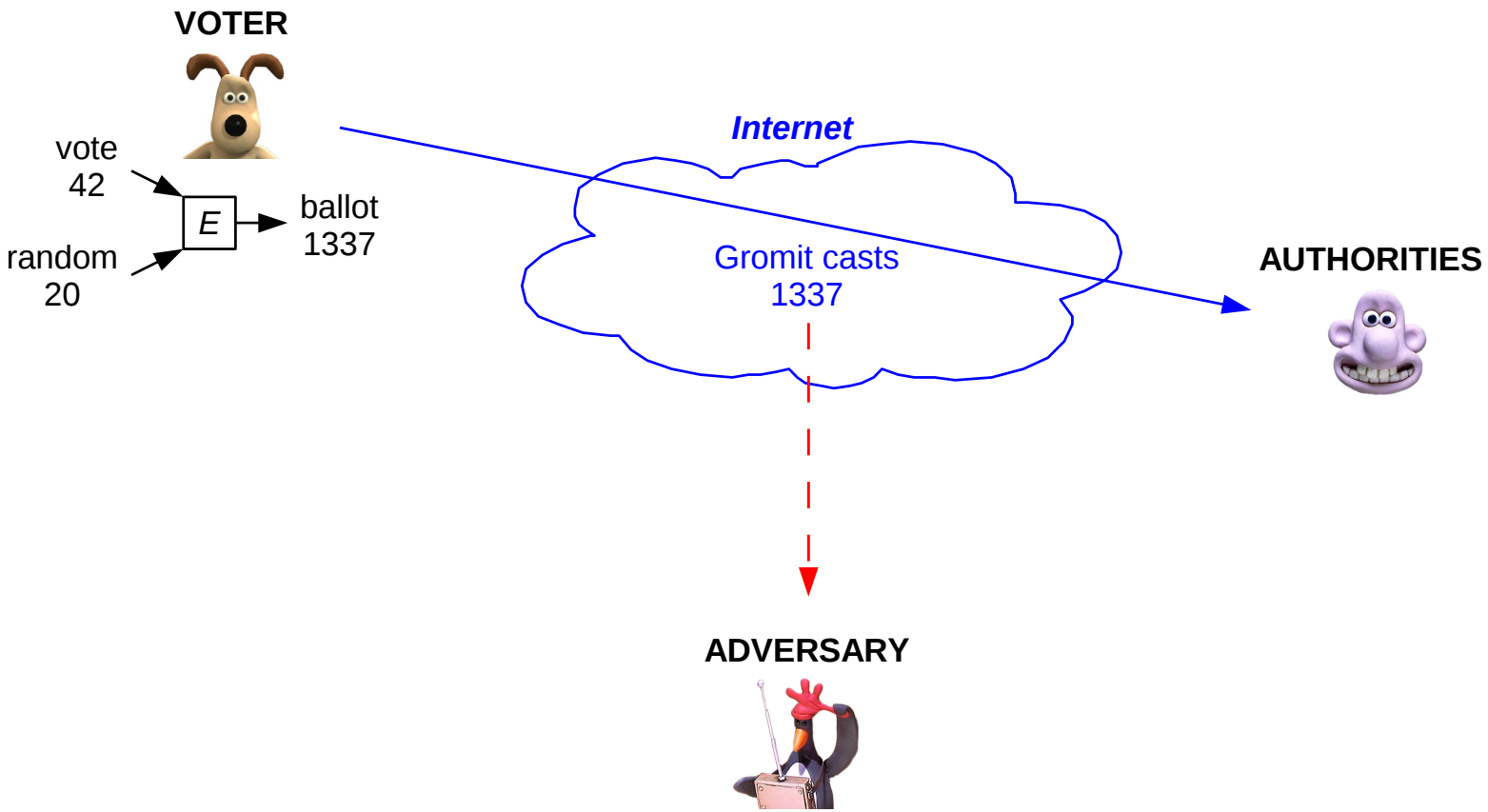
Example: A Flawed Scheme

- Hypothetical voting scheme: voters and authorities only communicate via the Internet



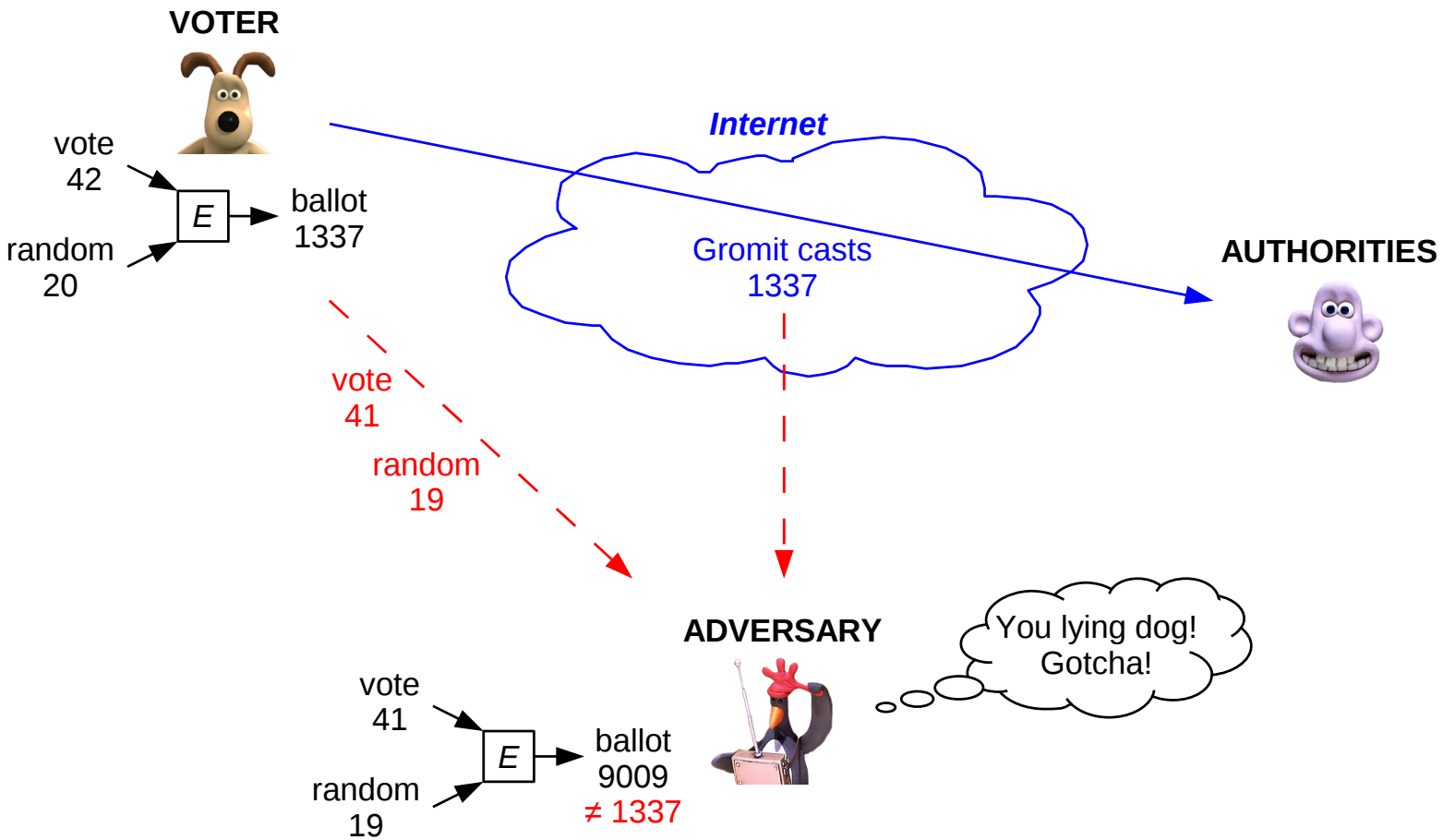
Example: A Flawed Scheme

- Hypothetical voting scheme: voters and authorities only communicate via the Internet



Example: A Flawed Scheme

- Hypothetical voting scheme: voters and authorities only communicate via the Internet

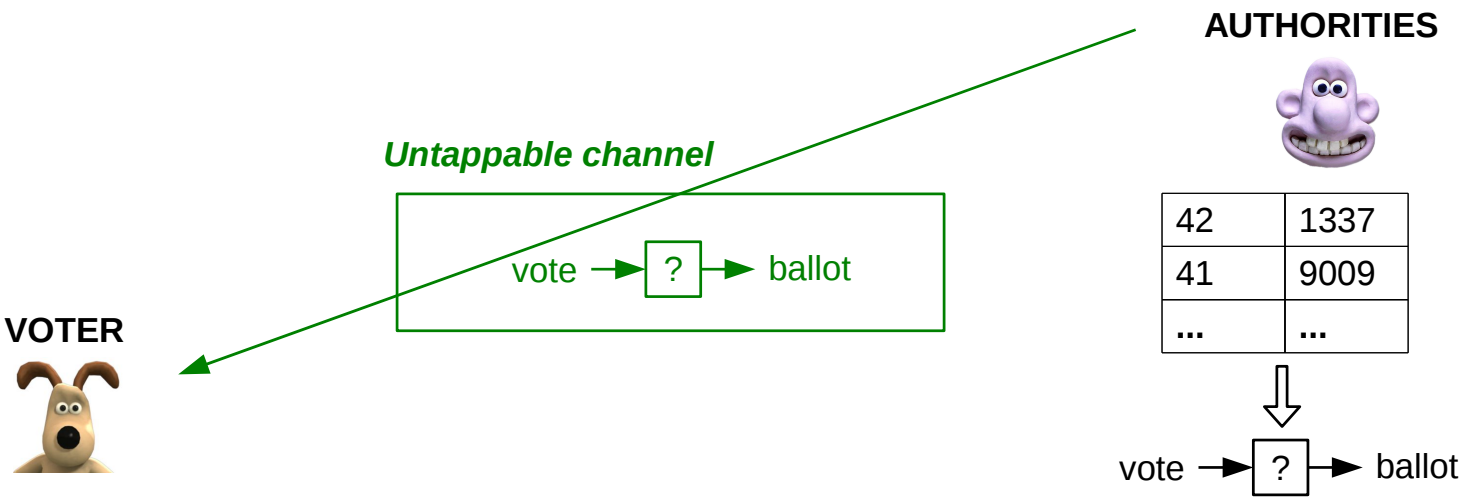


1. Untappable Channels Approach

- Untappable channels: adversary cannot intercept messages

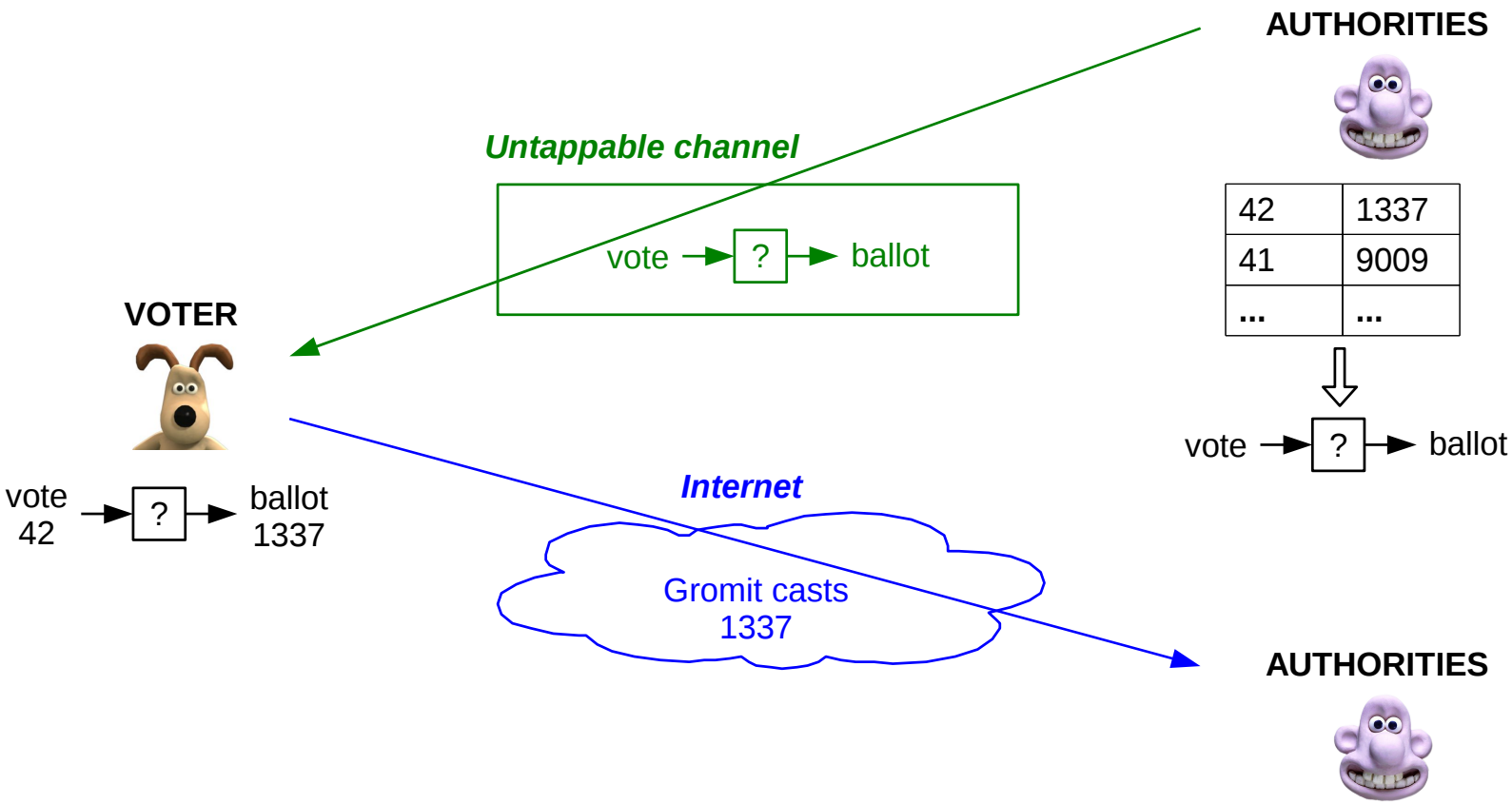
1. Untappable Channels Approach

- Untappable channels: adversary cannot intercept messages



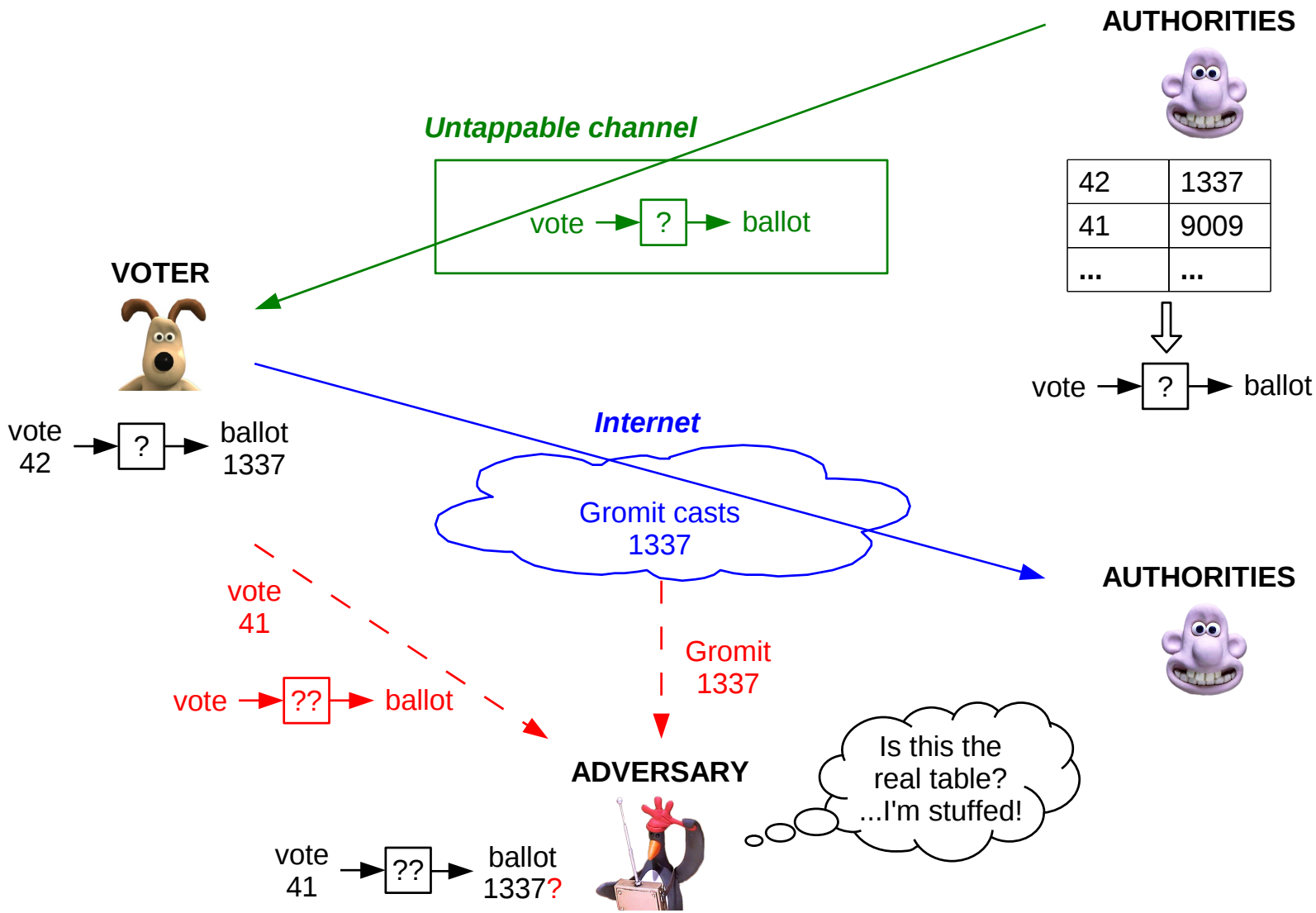
1. Untappable Channels Approach

- Untappable channels: adversary cannot intercept messages



1. Untappable Channels Approach

- Untappable channels: adversary cannot intercept messages



Problems with Untappable Channels

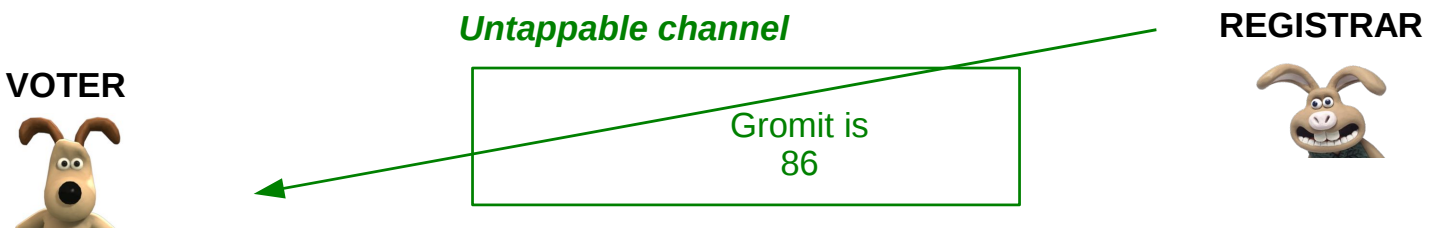
- Difficult to implement in practice
  - Internet susceptible to eavesdropping by well-funded adversary
- Resolving disputes
  - If voter claims authority is dishonest during the election, who is lying?
- Distributing trust among multiple authorities
  - Voter must know identity of at least one trusted authority to lie safely
  - Voter will be caught out if lying about messages from a corrupt authority
  - $\Rightarrow$ Typically have to assume no authorities collude with the adversary to bribe or coerce voters

2. Anonymous Channels Approach

- Anonymous channels: adversary cannot identify senders

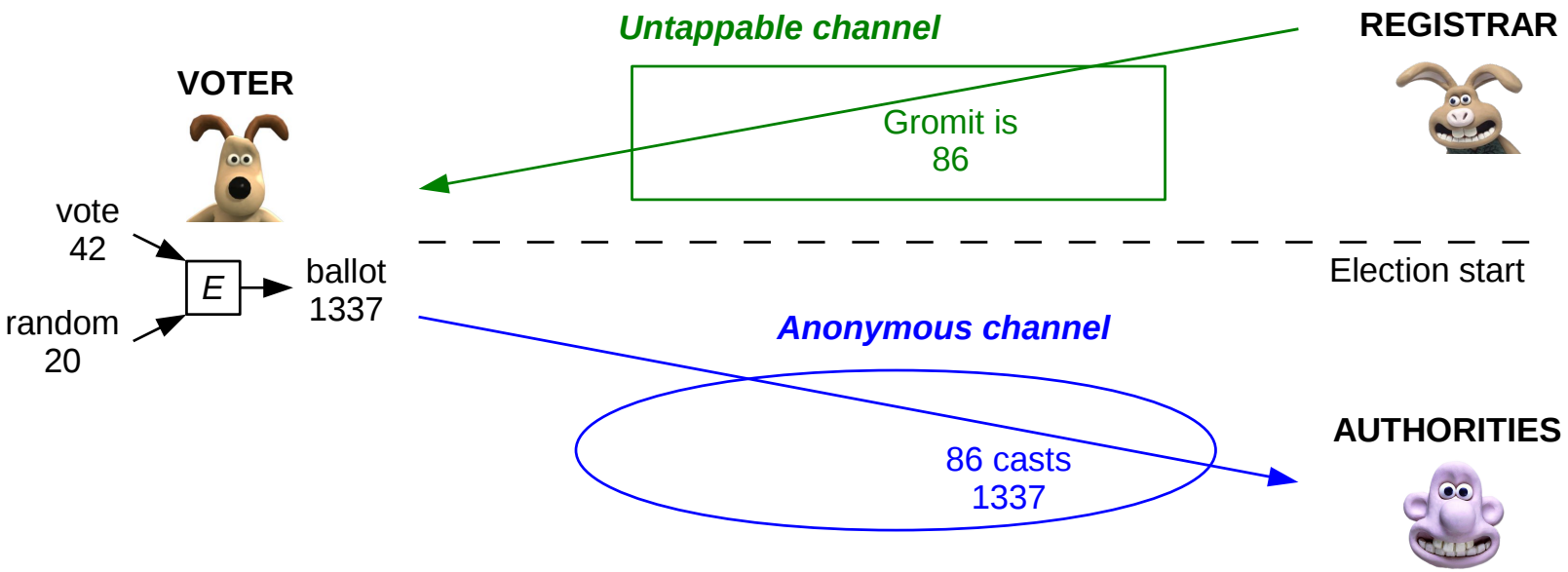
2. Anonymous Channels Approach

- Anonymous channels: adversary cannot identify senders



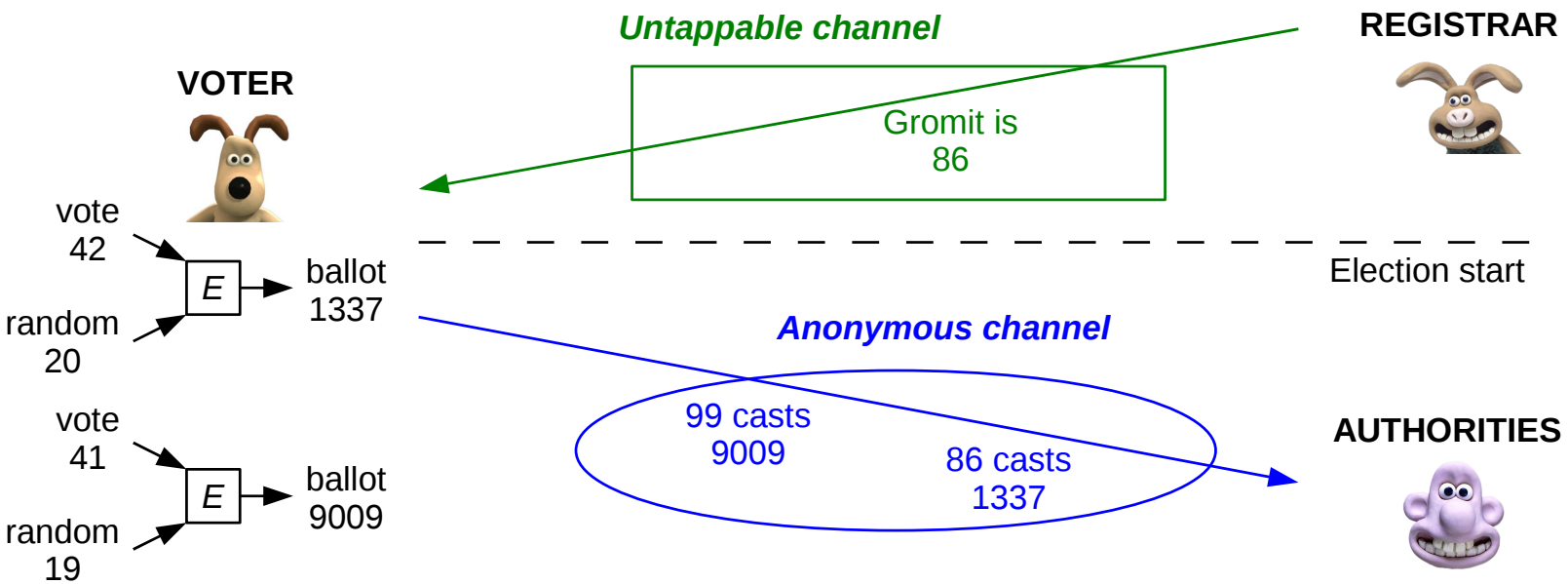
2. Anonymous Channels Approach

- Anonymous channels: adversary cannot identify senders



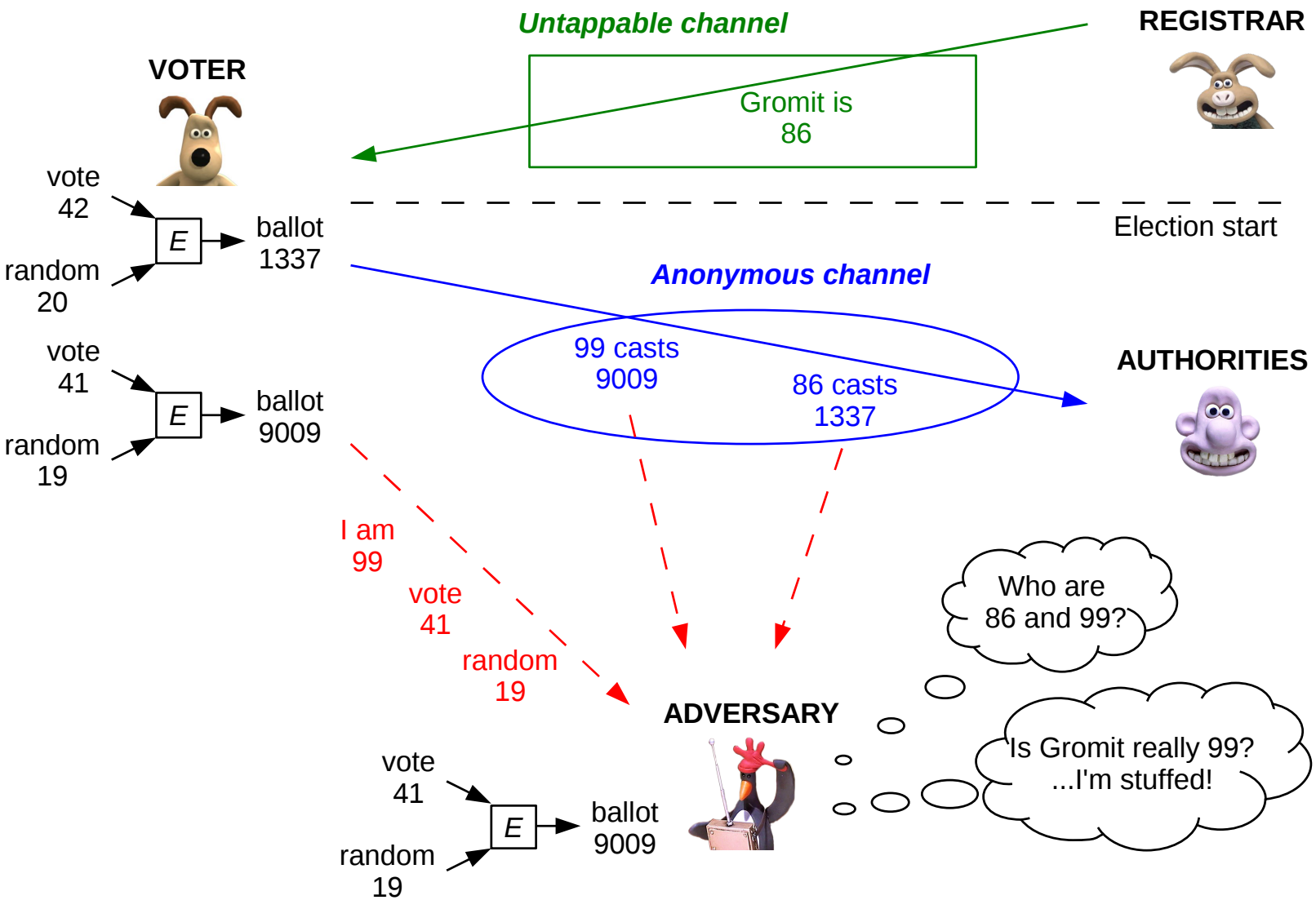
2. Anonymous Channels Approach

- Anonymous channels: adversary cannot identify senders



2. Anonymous Channels Approach

- Anonymous channels: adversary cannot identify senders



Problems with Anonymous Channels

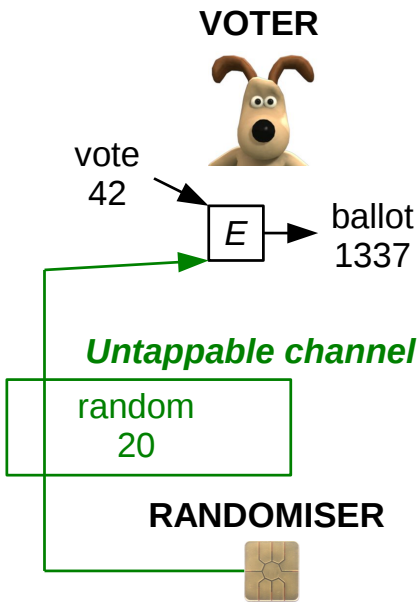
- Difficult to implement in practice
  - Hard to guarantee anonymity over Internet
  - Eg mix-nets still require untappable channels between voters and mix-net
- Problems remain with offline untappable channels
  - Resolving disputes
  - Distributing trust

3. Trusted Randomisers Approach

- Trusted randomisers: generate secret randomness

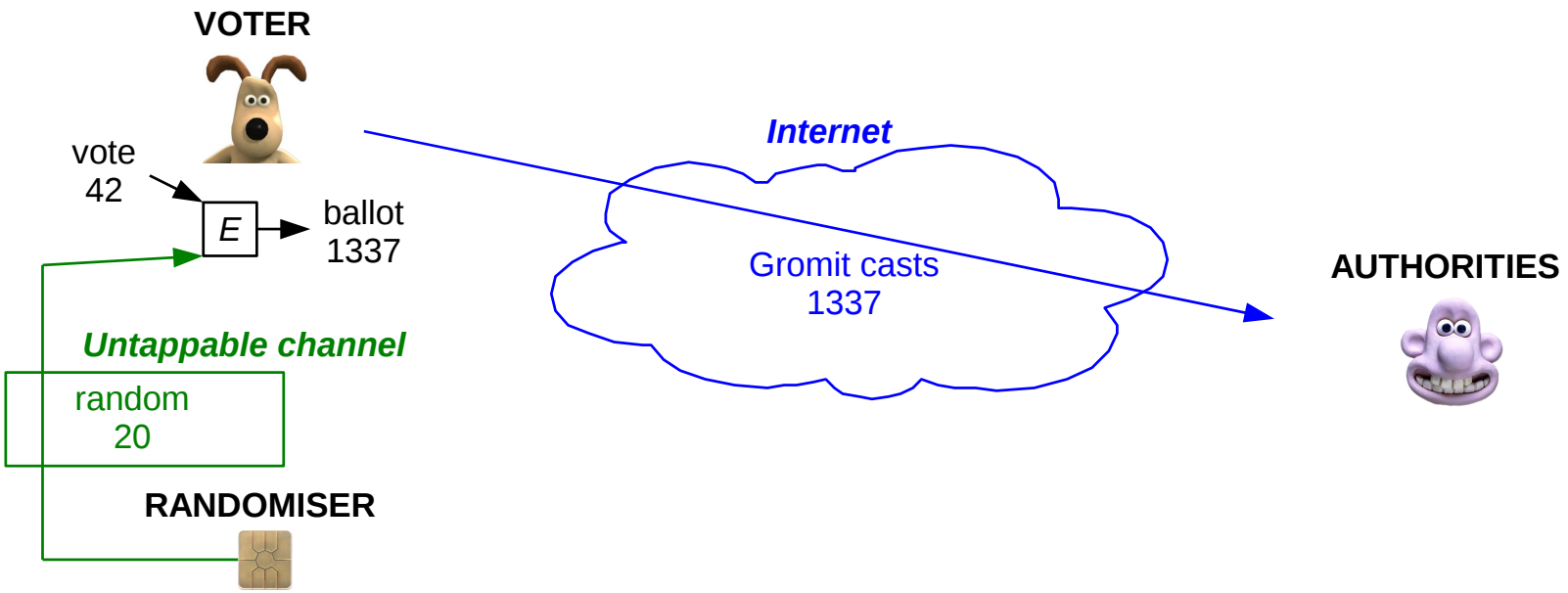
3. Trusted Randomisers Approach

- Trusted randomisers: generate secret randomness



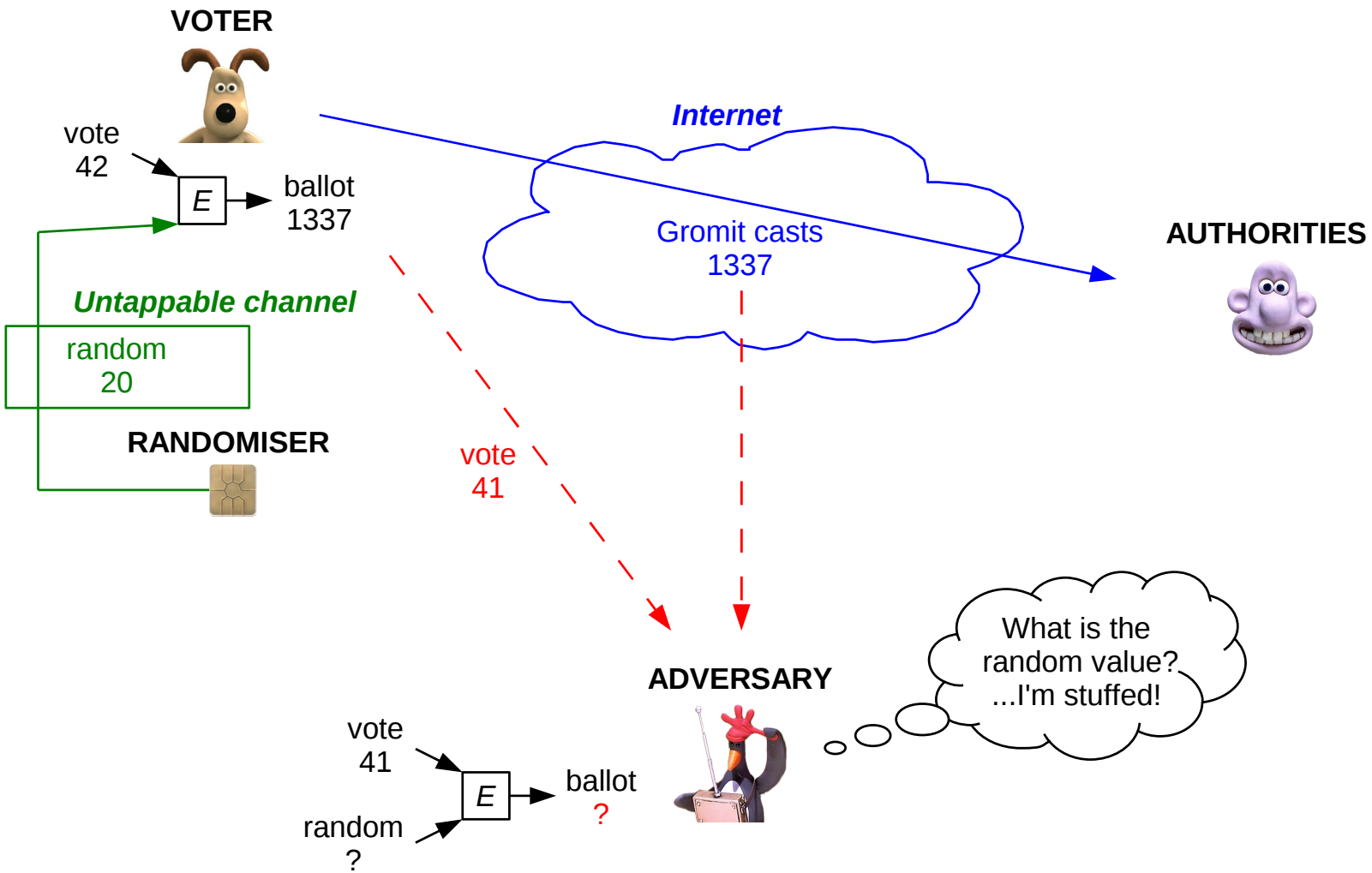
3. Trusted Randomisers Approach

- Trusted randomisers: generate secret randomness



3. Trusted Randomisers Approach

- Trusted randomisers: generate secret randomness



Problems with Trusted Randomisers

- A lot of trust involved
  - Hard to guarantee local channel is untappable
  - Smart cards are tamper-resistant not tamper-proof
  - Single point of failure

Masked Ballot Voting Scheme

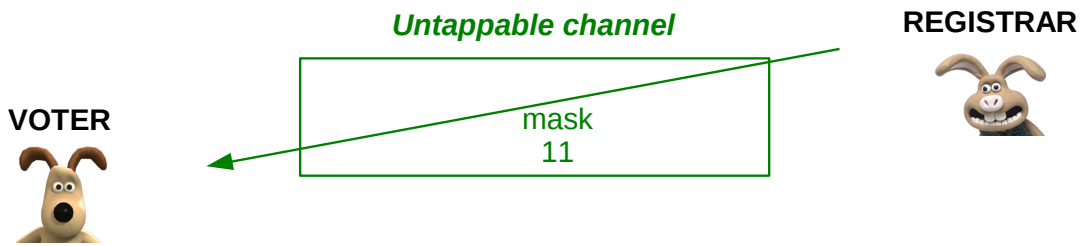
Approach

- How to avoid strong assumptions during the election?
  - Voters and authorities can only communicate via the Internet
  - Adversary can intercept all messages
- $\Rightarrow$ Voter must construct ballot without any assistance during the election
  - $\Rightarrow$ Adversary can verify the voter's private data against eavesdropped ballot
  - $\Rightarrow$ Private data must appear to correspond with any possible vote
- How does a voter indicate the actual vote?
  - Vote must depend on secret information obtained before the election

Masked Ballot Voting

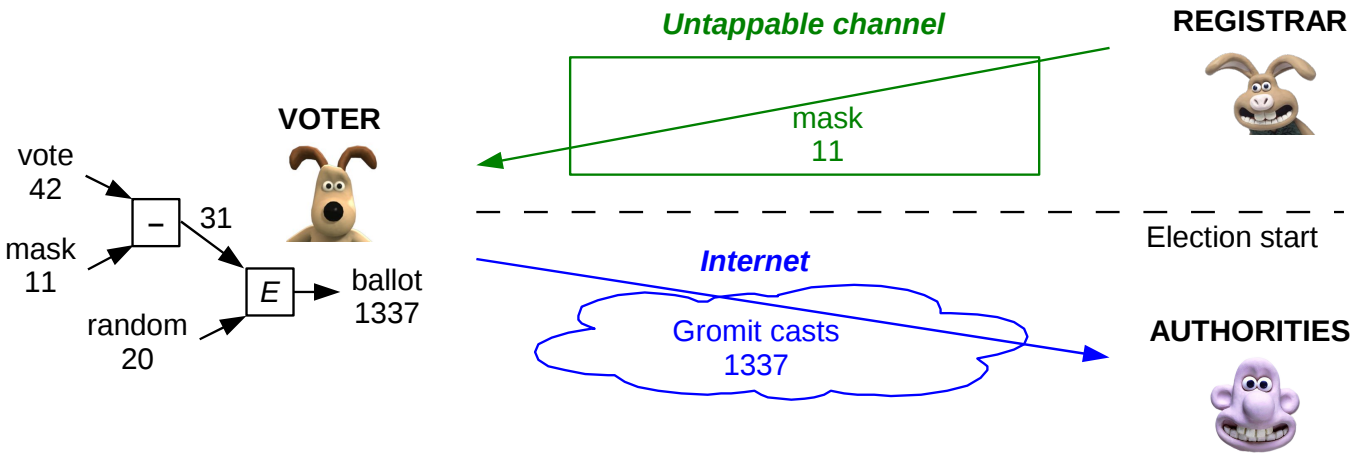
- Assumption: untappable channels available only before the election (offline registration stage)
  - All communication during the election is posted to authenticated bulletin board via Internet
- Purely a voting scheme
  - The output is an encrypted vote for each voter
  - Generic: independent of the vote encoding
- Subsequent counting scheme calculates the result

Registration Stage



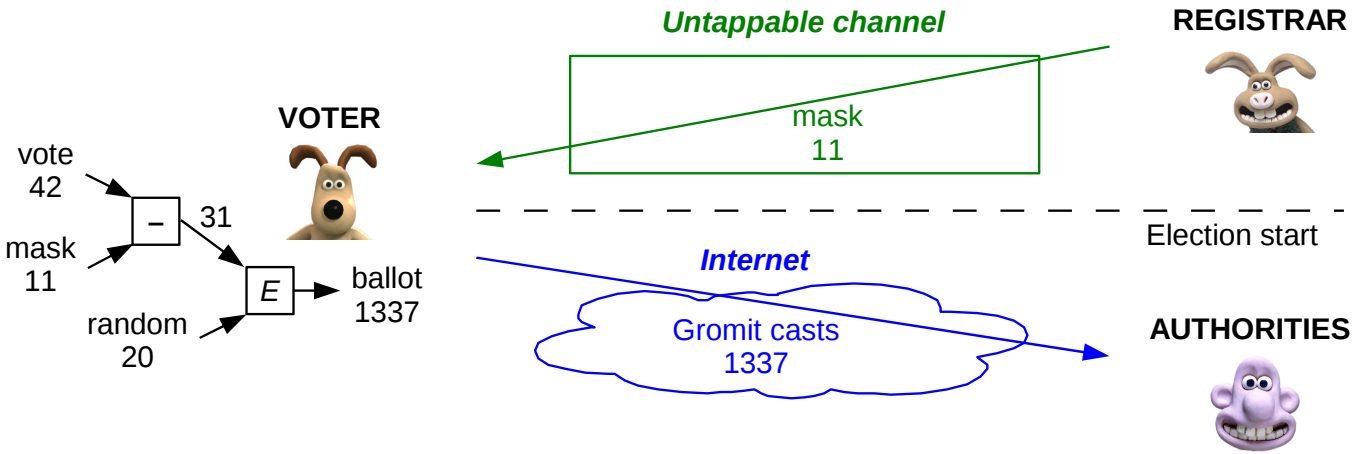
- A registrar provides each voter V with a secret mask
  1. Randomly select a mask m
  2. Encrypt $m \longrightarrow [\![m]\!]$
  3. Post $(V, [\![m]\!])$ to bulletin board
  4. Construct designated-verifier proof d that $[\![m]\!]$ is an encryption of m
  5. Send (m, d) to V via an **untappable channel**

Voting Stage



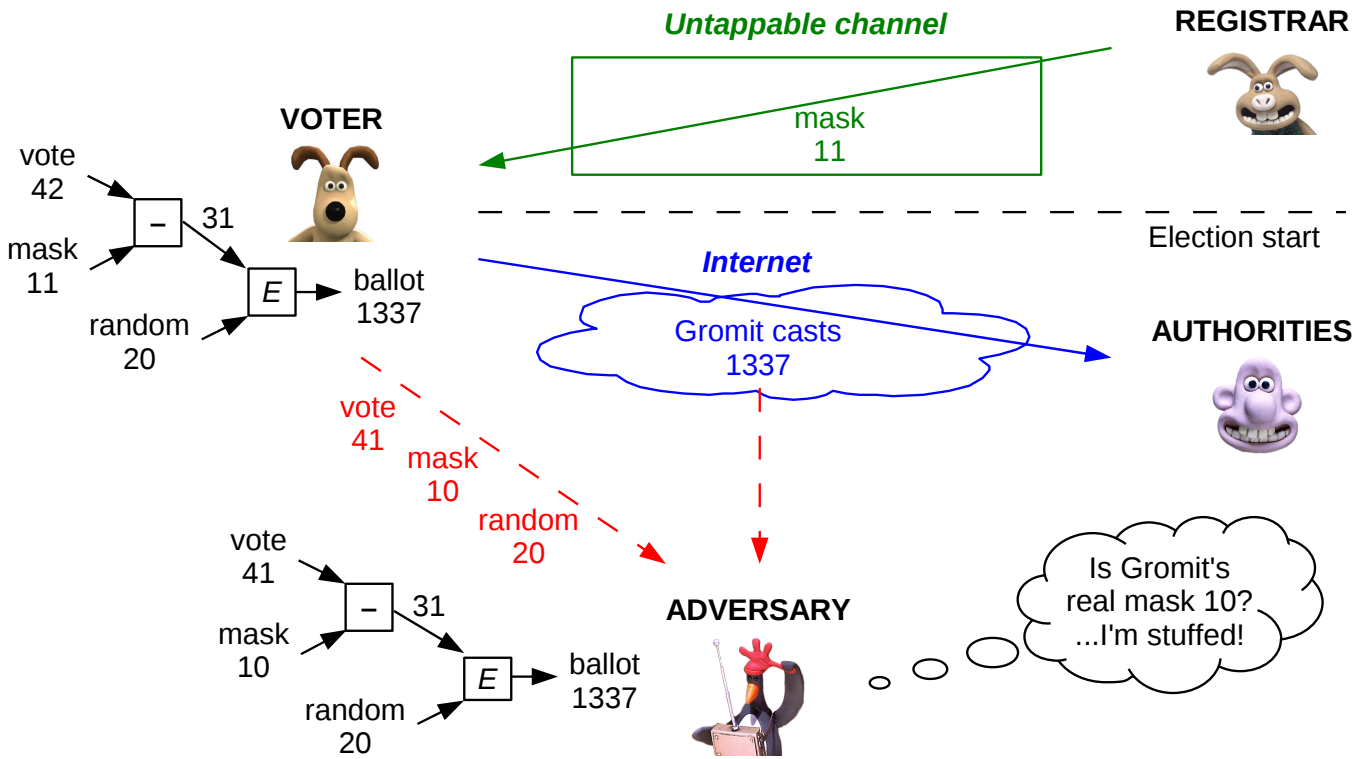
- A voter casts a masked ballot for a vote v using mask m
  1. Encrypt $(v - m) \longrightarrow [\![v - m]\!]$
  2. Construct proof p of plaintext knowledge
  3. Post $([\![v - m]\!], p)$ to the bulletin board via the Internet

Unmasking Stage



- For each voter, any party can unmask the ballot $[\![v - m]\!]$
  - Encrypt with threshold homomorphic cryptosystem, eg Paillier
  - Use additive homomorphism to combine $[\![m]\!]$ posted by the registrar and $[\![v - m]\!]$ posted by the voter
  - $[\![v - m]\!] \boxplus [\![m]\!] = [\![v]\!]$

Thwarting the Adversary



- Gromit cannot lie about input 31 $(v - m)$
  - But can lie about m and hence v

1. Attacks after ballot is cast
2. Attacks before ballot is cast

Proving Receipt-Freeness

- Moran and Naor's simulation-based model
  - Receipt-free against an adaptive adversary
- Ideal world captures properties of ideal voting protocol
  - Only allows adversary to force voters to abstain or vote randomly
  - Simulate the real protocol
  - $\Rightarrow$ Real protocol is as receipt-free as ideal protocol
- Voting protocol has a coercion-resistance strategy
  - Describes how voters thwart the adversary's instructions

Discussion

Limitations of Masked Ballot Assumptions

- Secret information (mask) sent before election cannot be re-used
  - Less convenient for voters
- Voters cannot provide proofs of vote validity
  - May require extra work for authorities to remove invalid votes before the counting
- Voters can still prove if they abstained or voted randomly
  - Coercion-resistance property requires anonymous channels
  - So only receipt-freeness is achievable

Summary

- All approaches to receipt-freeness use untappable channels to protect some secret information
  - Different trade-offs
- Masked Ballot Voting Scheme achieves receipt-freeness with a more practical assumption during the election
  - Only relies on standard cryptographic components during the election
  - Shifts problematic assumptions to before the election
- Many good cryptographic solutions
  - Biggest remaining problem is to resolve practical issues
  - Eg authentication, DOS, malware, shoulder-surfing