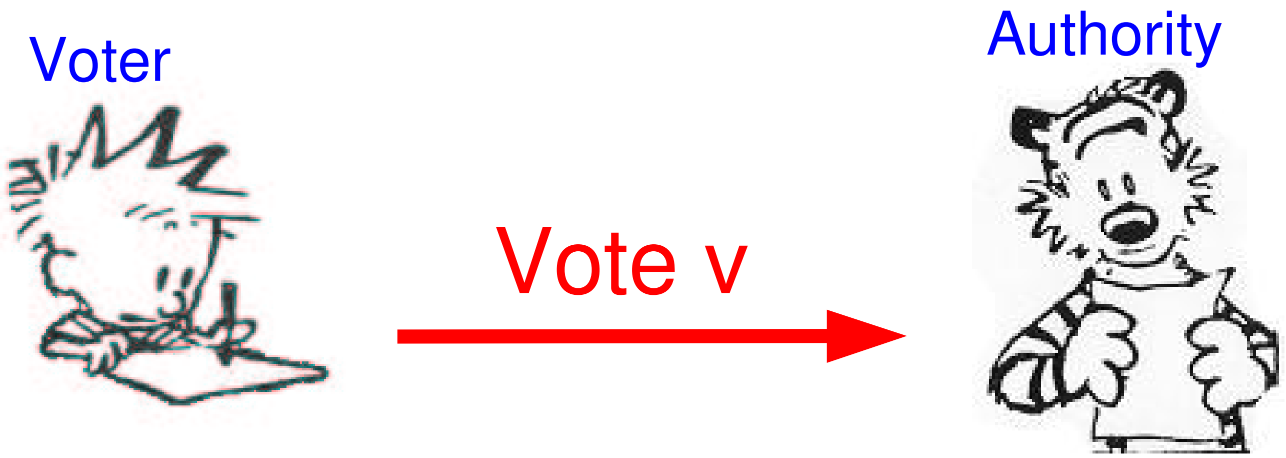
Electronic Voting in the Standard Model

Semesterarbeit
SS03



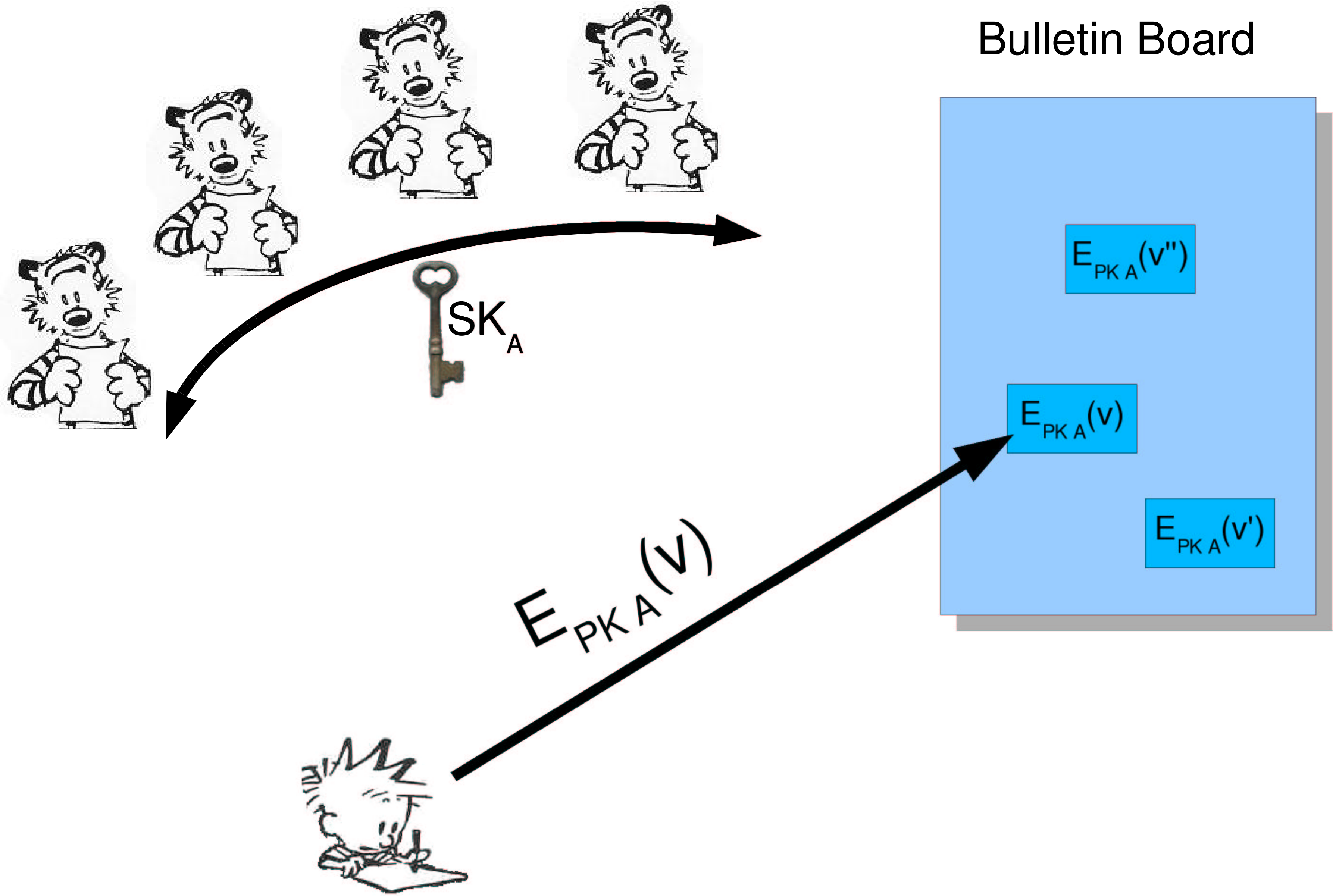
Voter

Vote v

Authority

Thomas Briner

Betreuung: Martin Hirt



Bulletin Board

$E_{PK\ A}(v'')$

$E_{PK\ A}(v)$

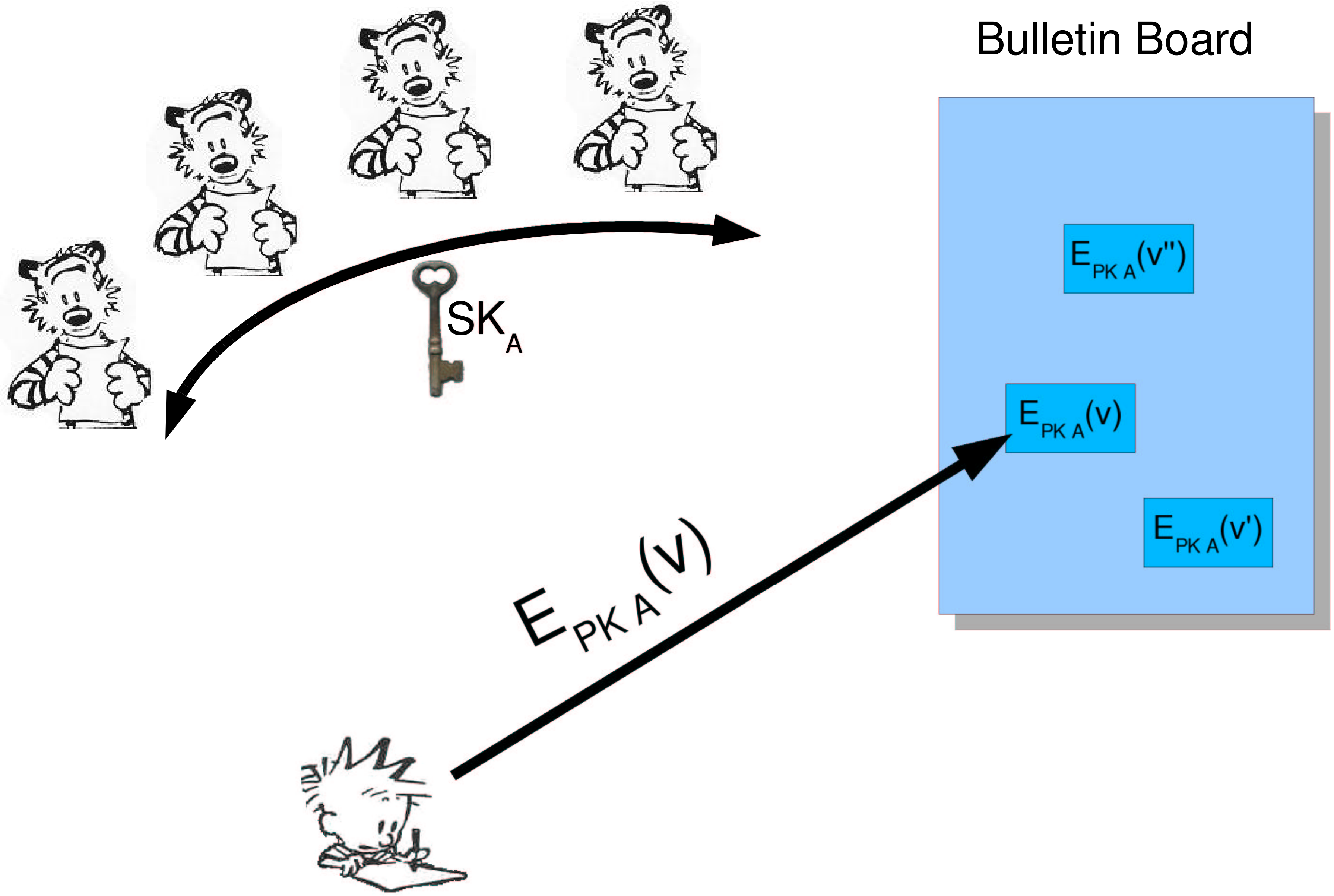
$E_{PK\ A}(v')$

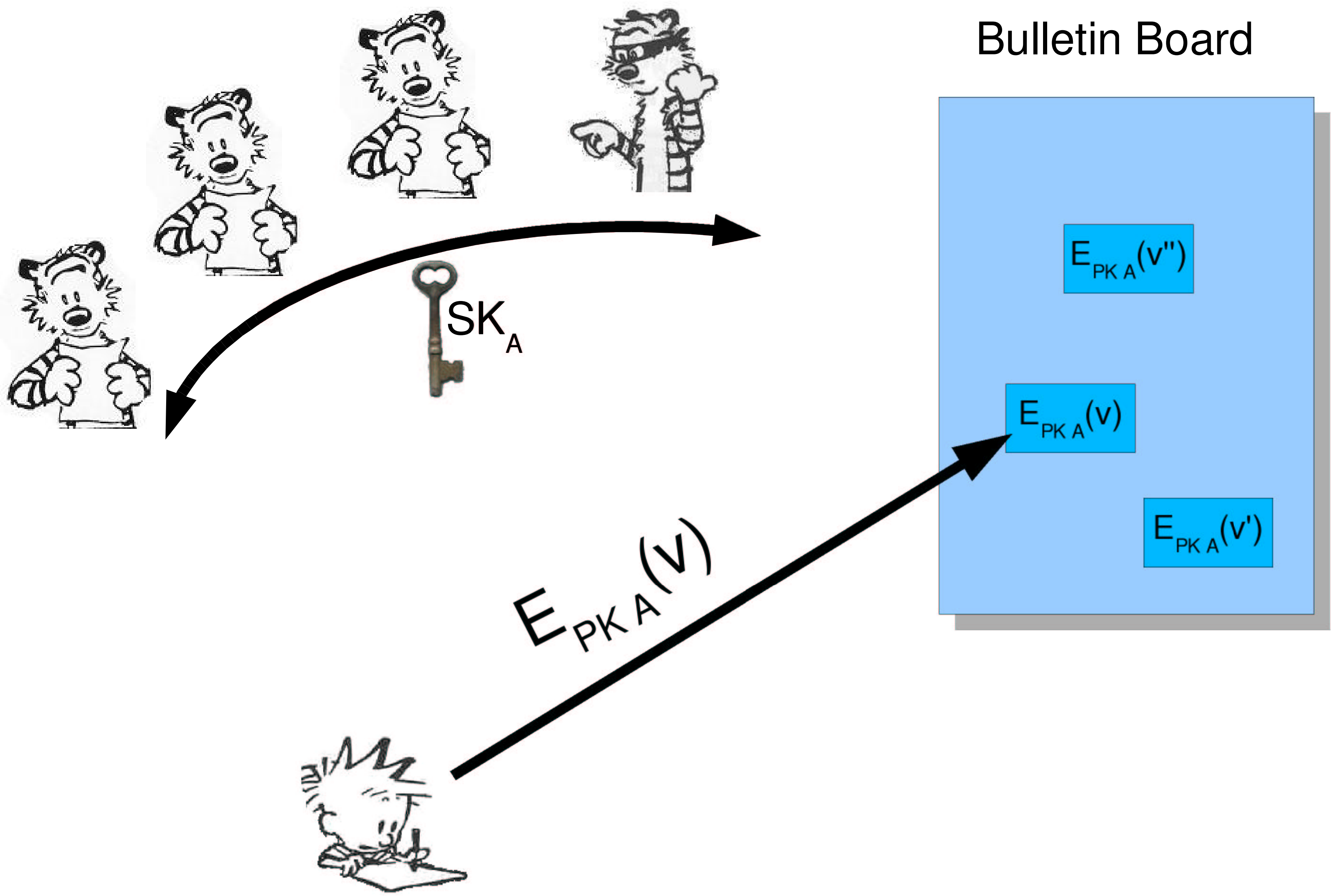
SK_A

$E_{PK\ A}(v)$

Homomorphic Encryption

$$E(v_1) \oplus E(v_2) = E(v_1 + v_2)$$


Bulletin Board
$E_{PK\ A}(v'')$
SK_A
$E_{PK\ A}(v)$
$E_{PK\ A}(v')$
$E_{PK\ A}(v)$



Bulletin Board

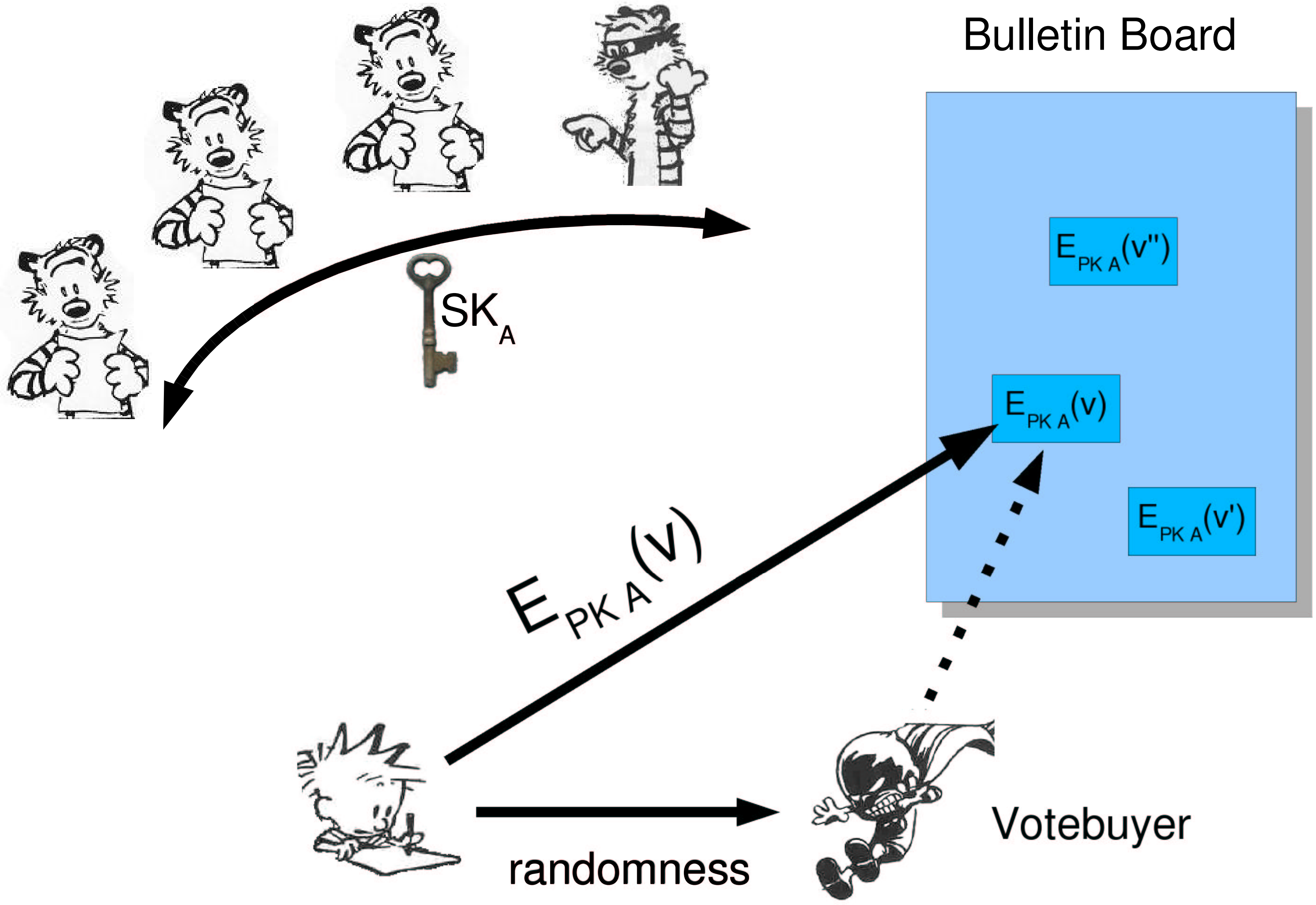
$E_{PK\ A}(v'')$

$E_{PK\ A}(v)$

$E_{PK\ A}(v')$

SK_A

$E_{PK\ A}(v)$



Bulletin Board

$E_{PK\ A}(v'')$

$E_{PK\ A}(v)$

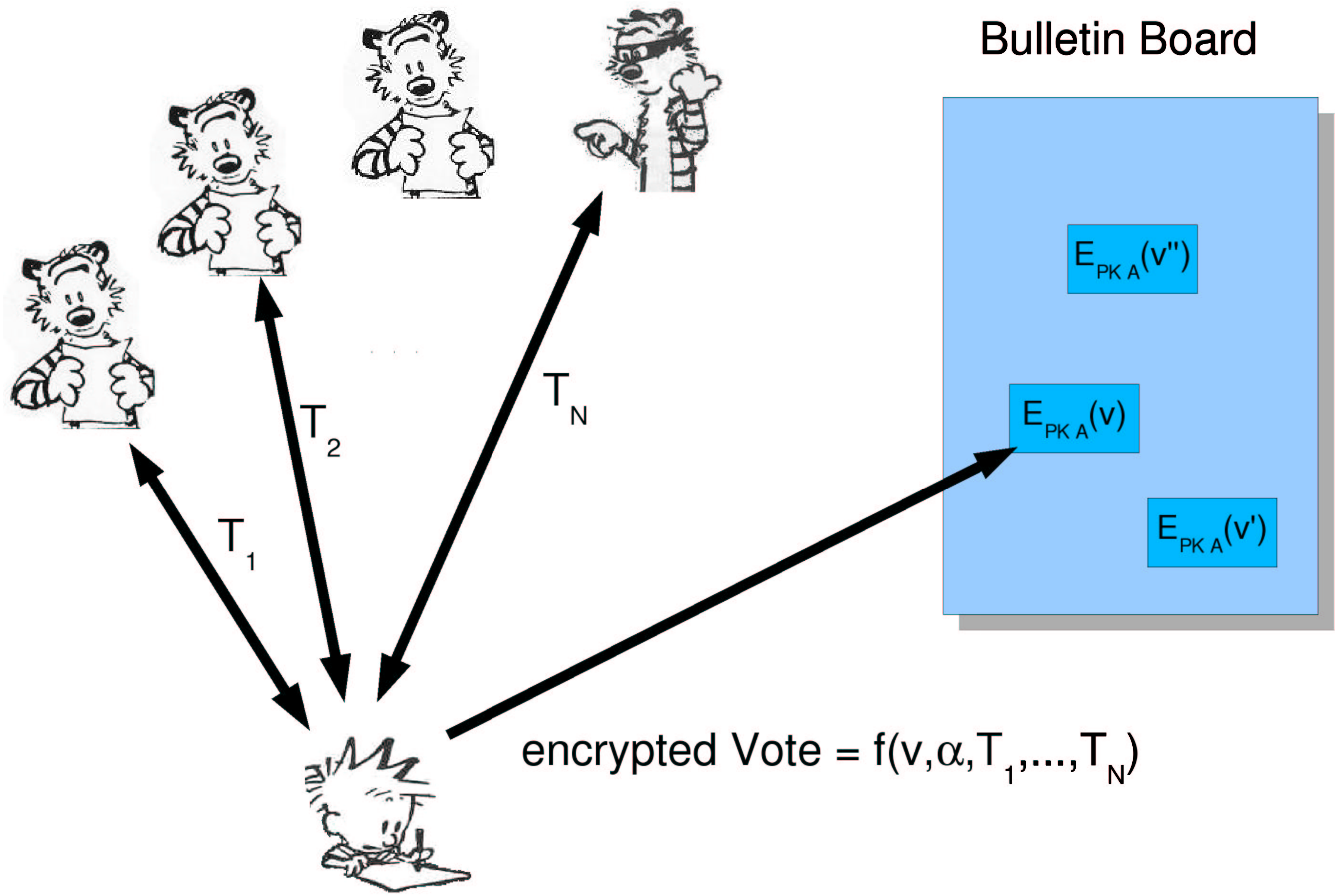
$E_{PK\ A}(v')$

SK_A

$E_{PK\ A}(v)$

randomness

Votebuyer



Bulletin Board

$E_{PK\ A}(v'')$

$E_{PK\ A}(v)$

$E_{PK\ A}(v')$

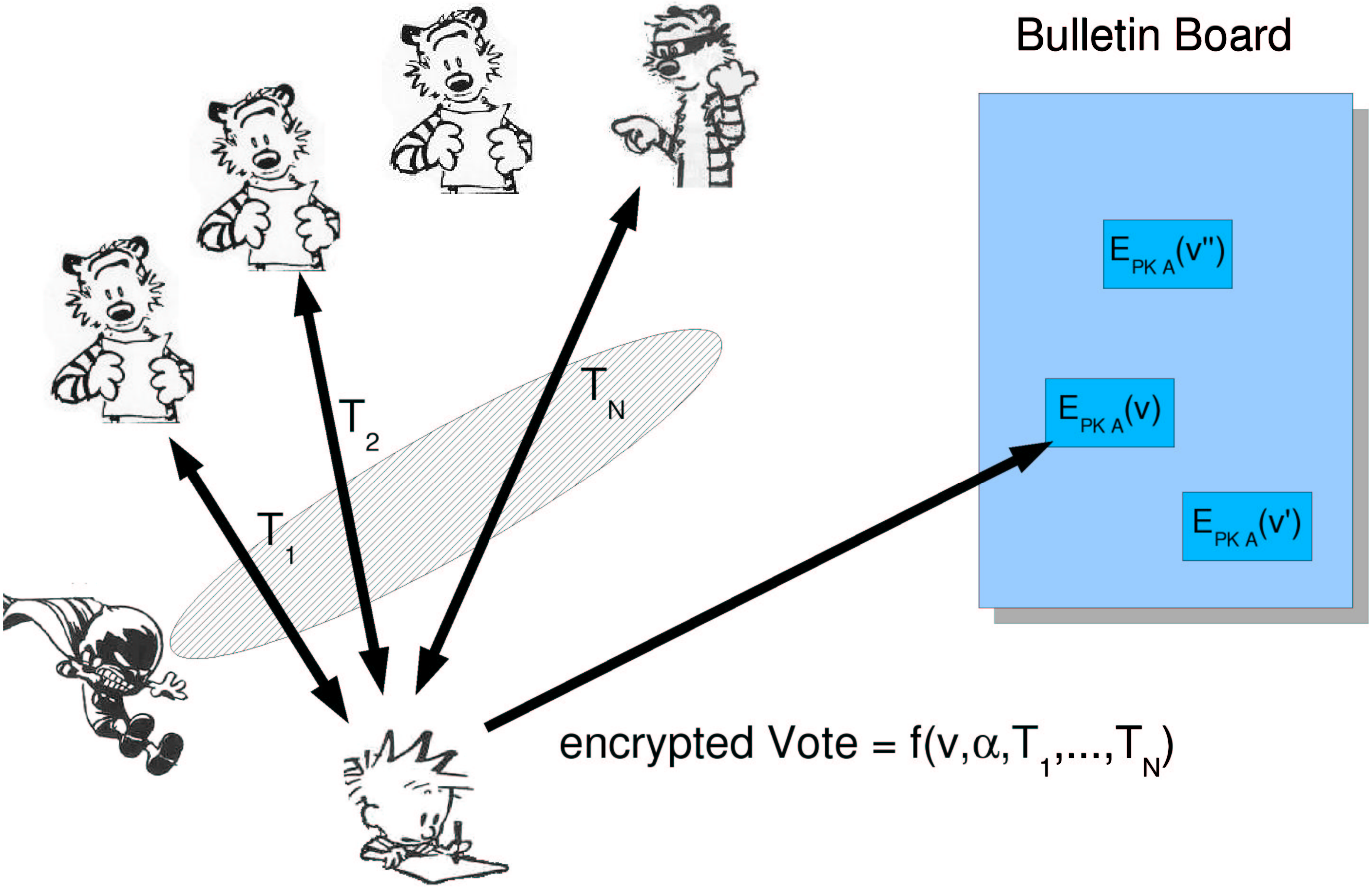
T_1

T_2

. . .

T_N

encrypted Vote = $f(v,\alpha,T_1,\ldots,T_N)$



Bulletin Board

$E_{PK\ A}(v'')$

$E_{PK\ A}(v)$

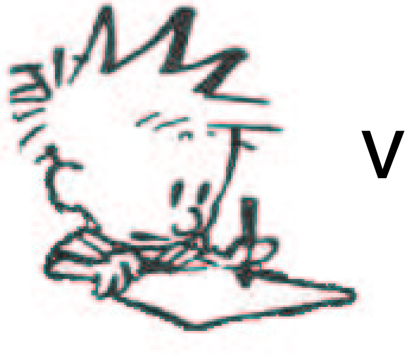
$E_{PK\ A}(v')$

T_1

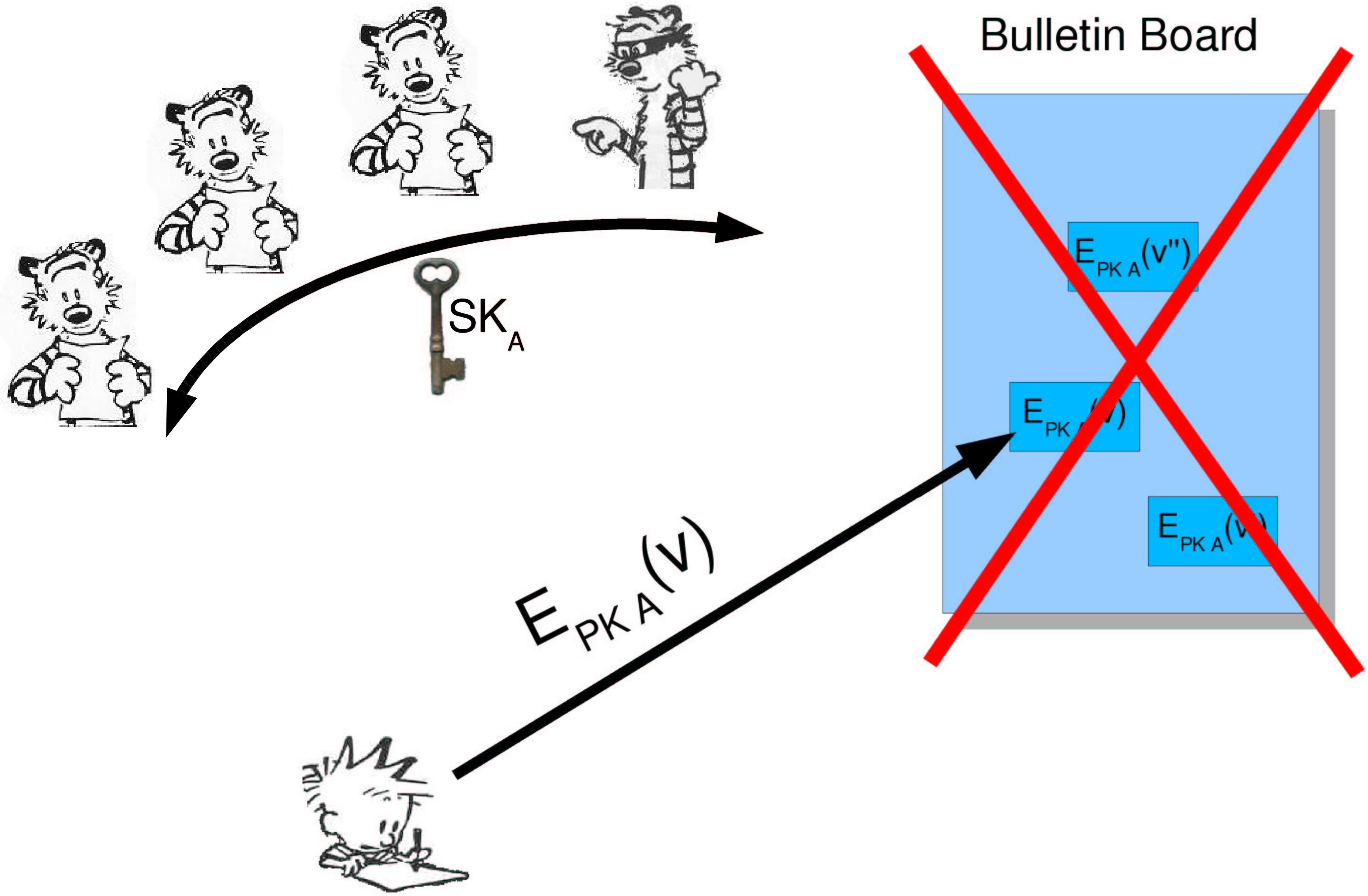
T_2

T_N

encrypted Vote = $f(v,\alpha,T_1,\ldots,T_N)$



$$v \xrightarrow{\text{homomorphic encryption}} e = E(v,\alpha) \xrightarrow{\text{blinding}} \bar{e}$$



Bulletin Board

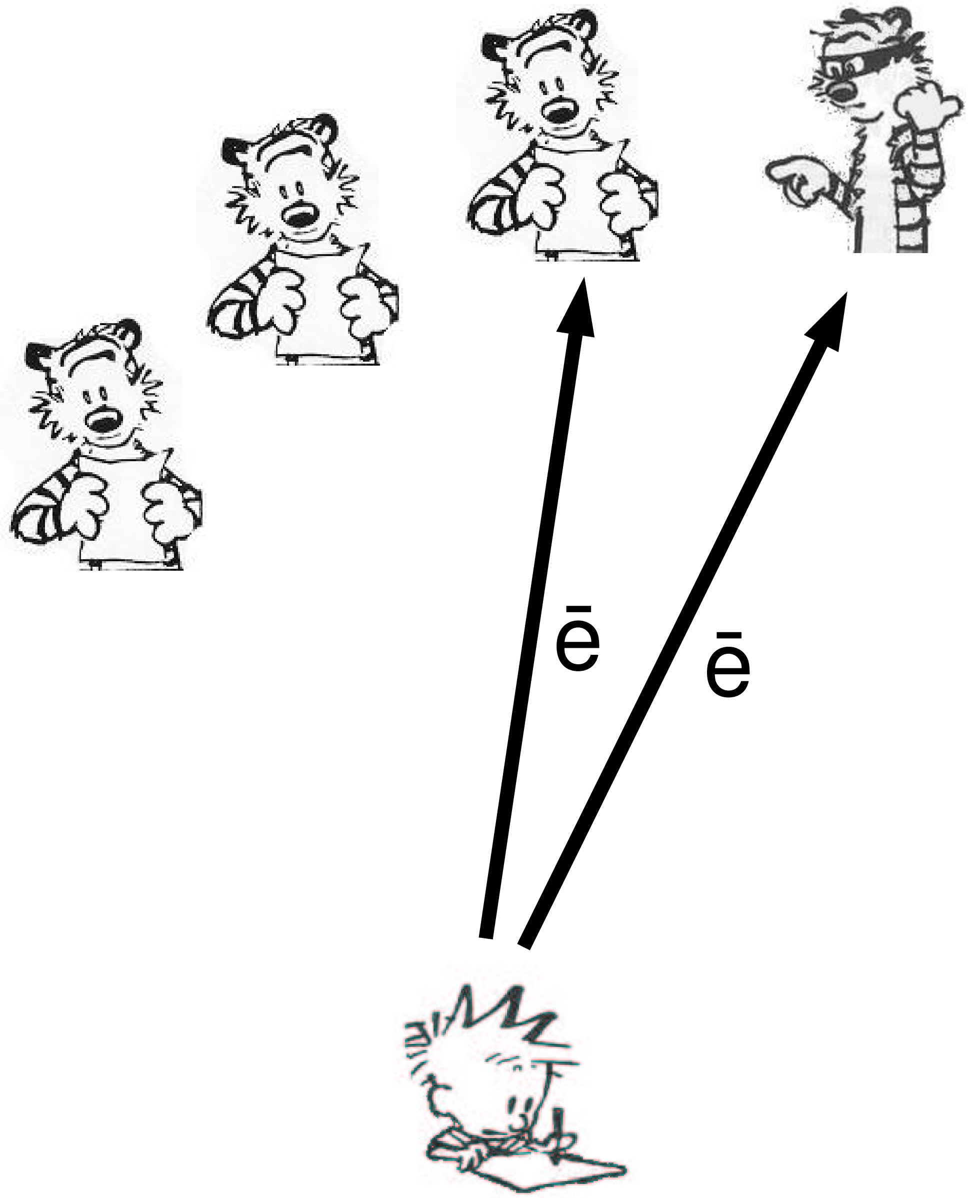
$E_{PK\,A}(v'')$

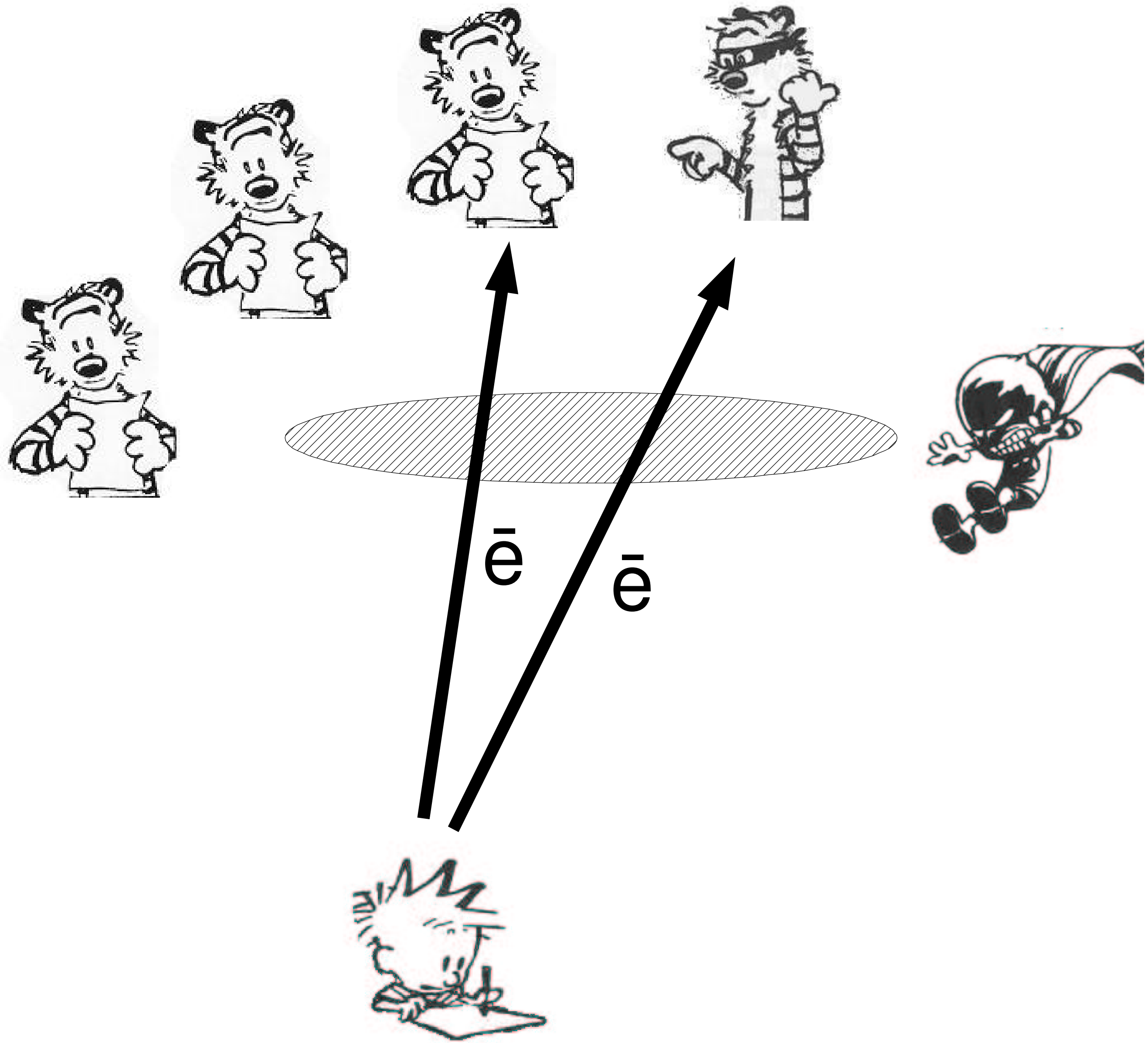
$E_{PK\,A}(v)$

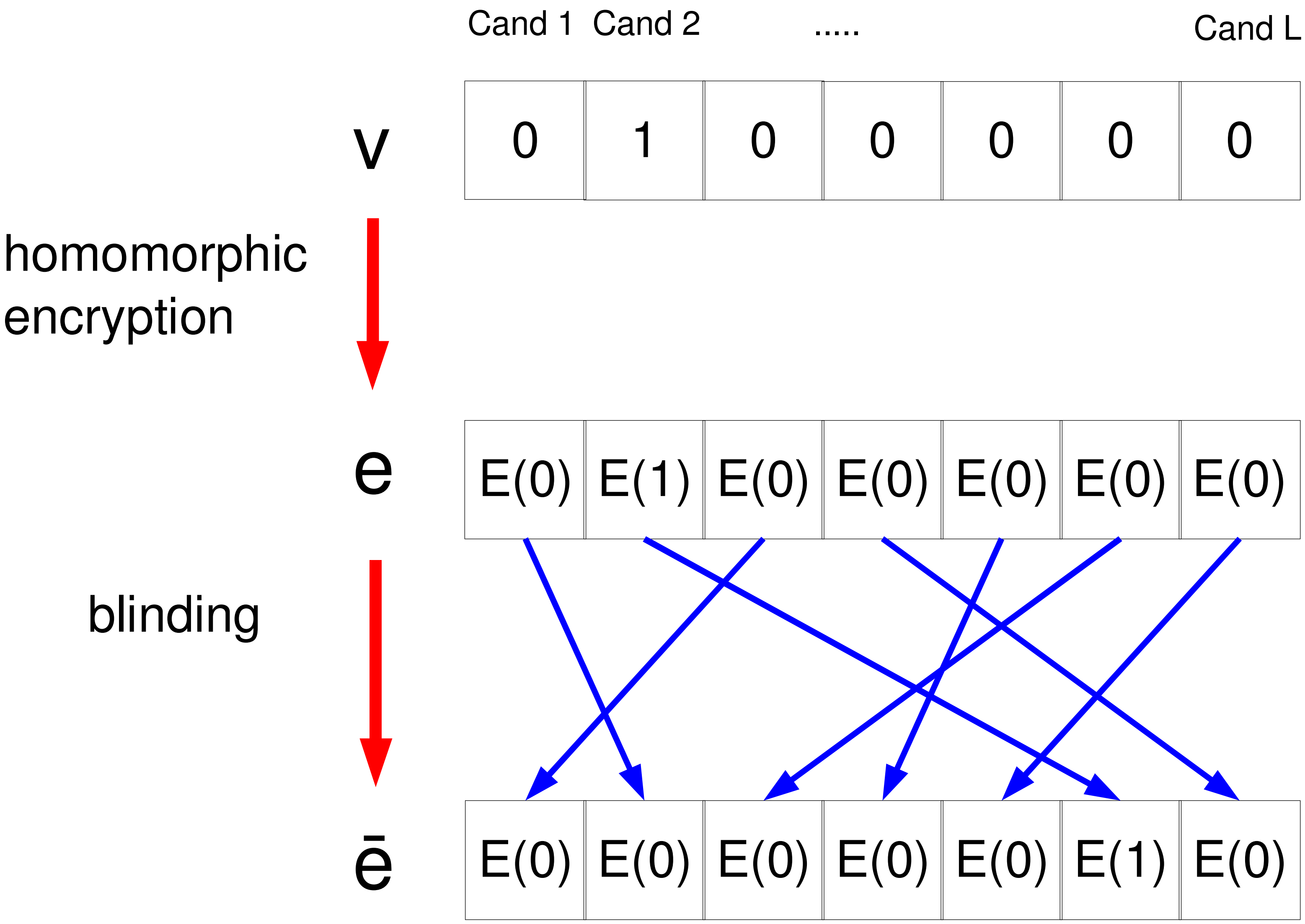
$E_{PK\,A}(v')$

SK_A

$E_{PK\,A}(v)$


ē
ē


ē
ē



Cand 1 Cand 2 ..... Cand L

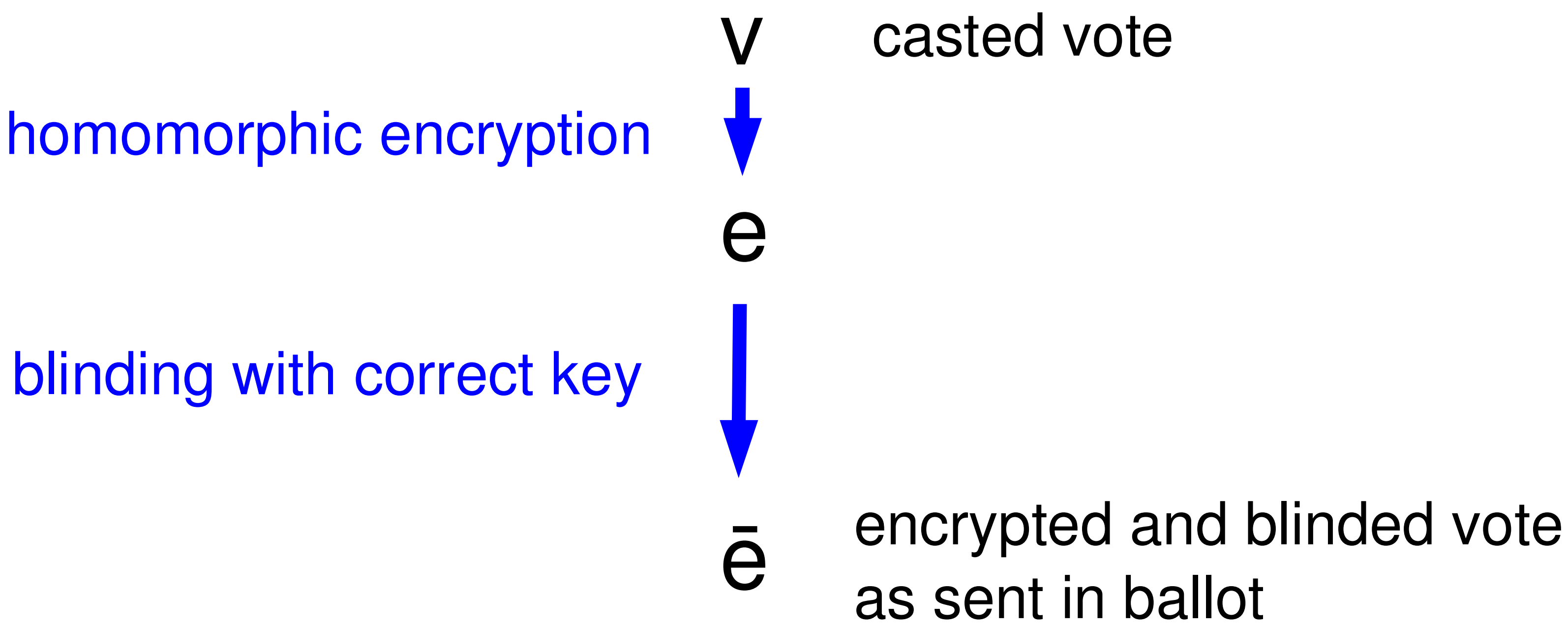
v 0 1 0 0 0 0 0

homomorphic encryption

e E(0) E(1) E(0) E(0) E(0) E(0) E(0)

blinding

ē E(0) E(0) E(0) E(0) E(0) E(1) E(0)



v casted vote

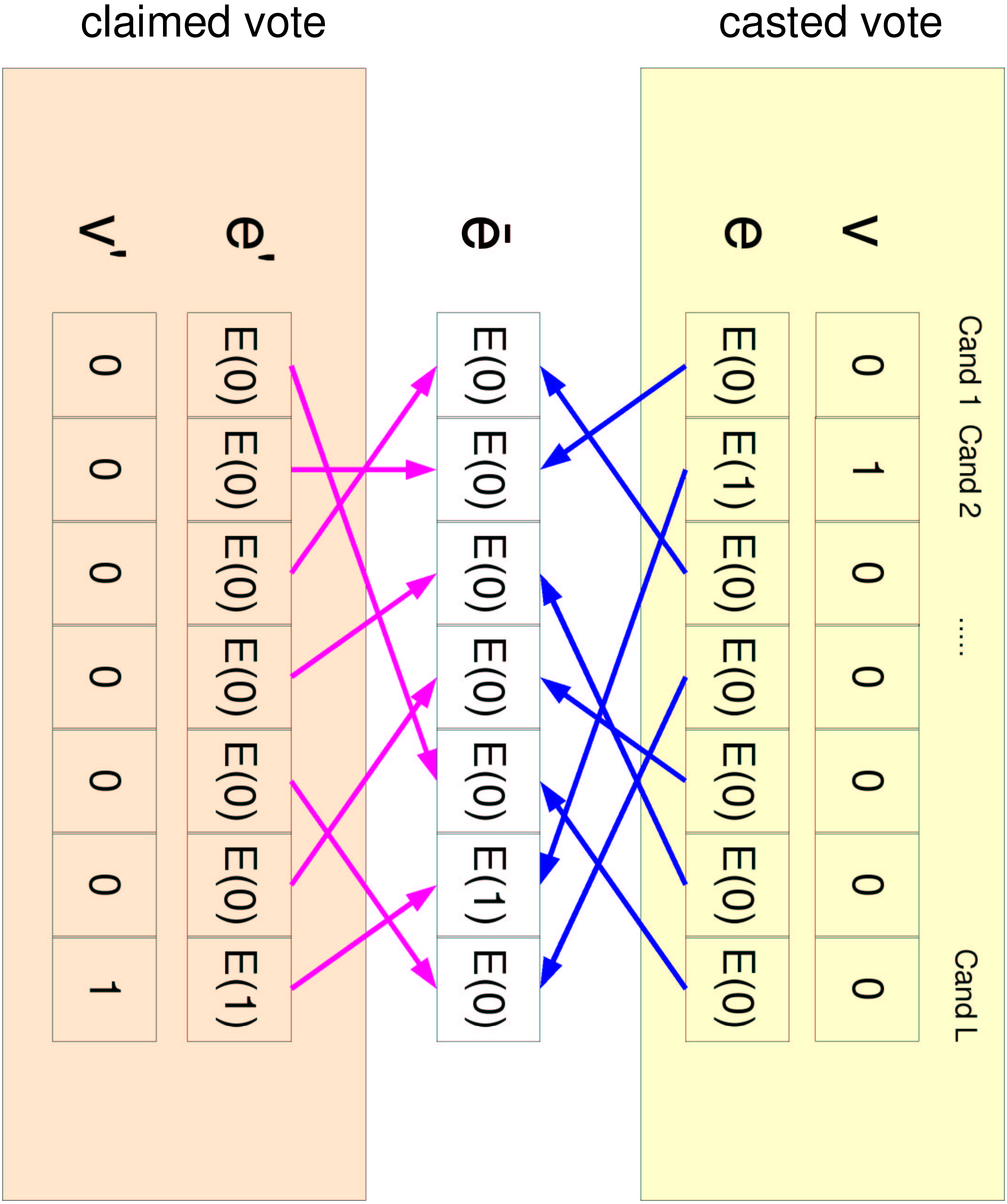
homomorphic encryption

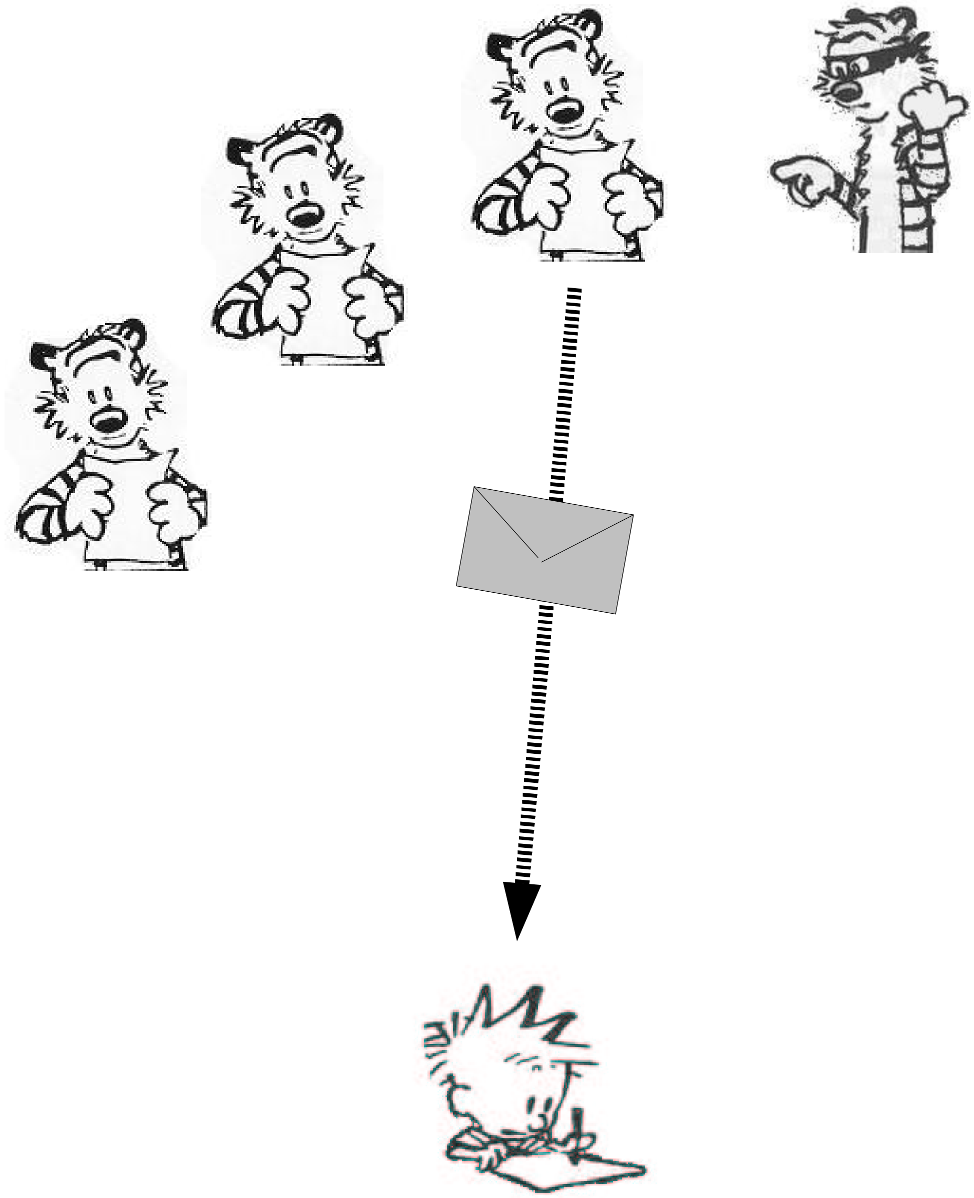
e

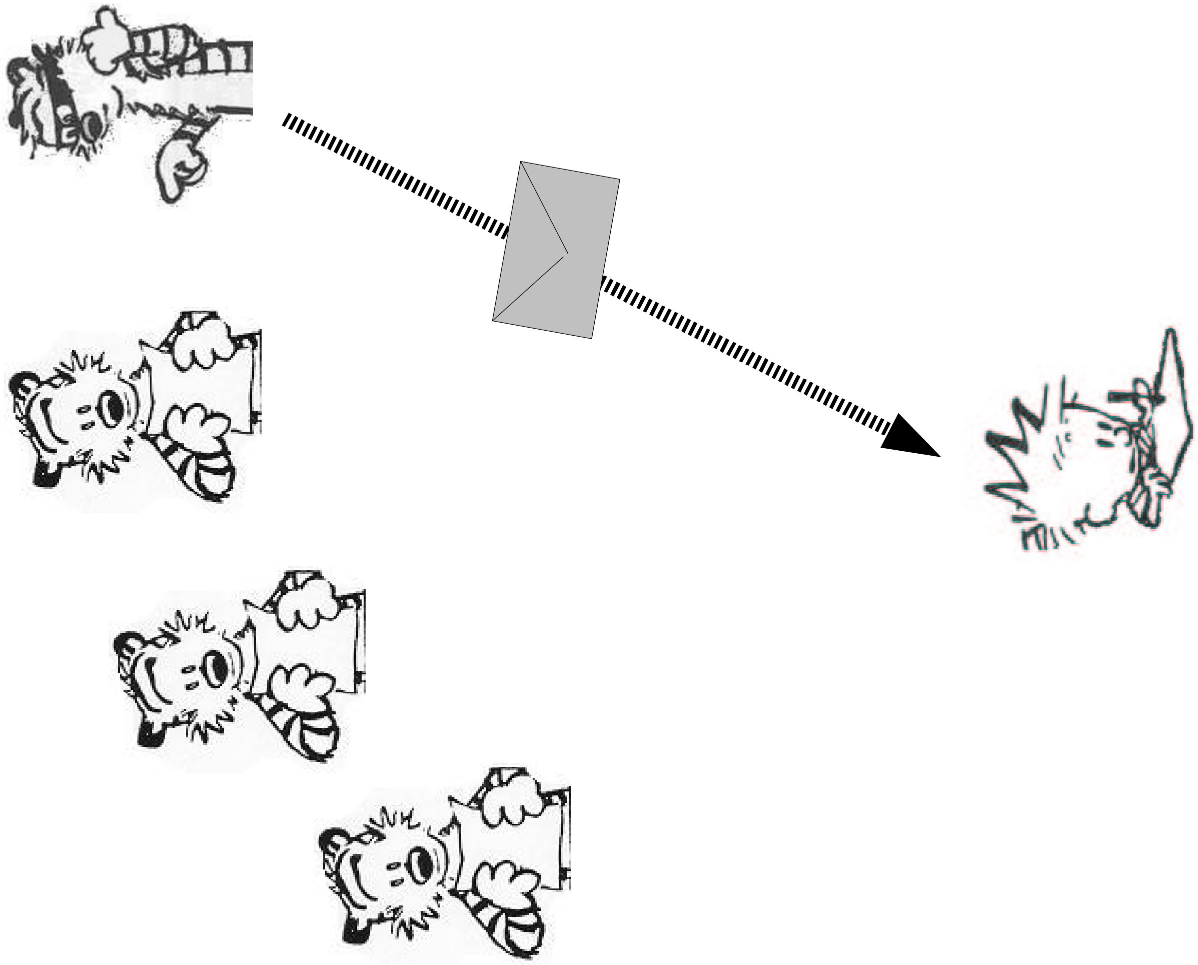
blinding with correct key

$\bar{e}$ encrypted and blinded vote as sent in ballot

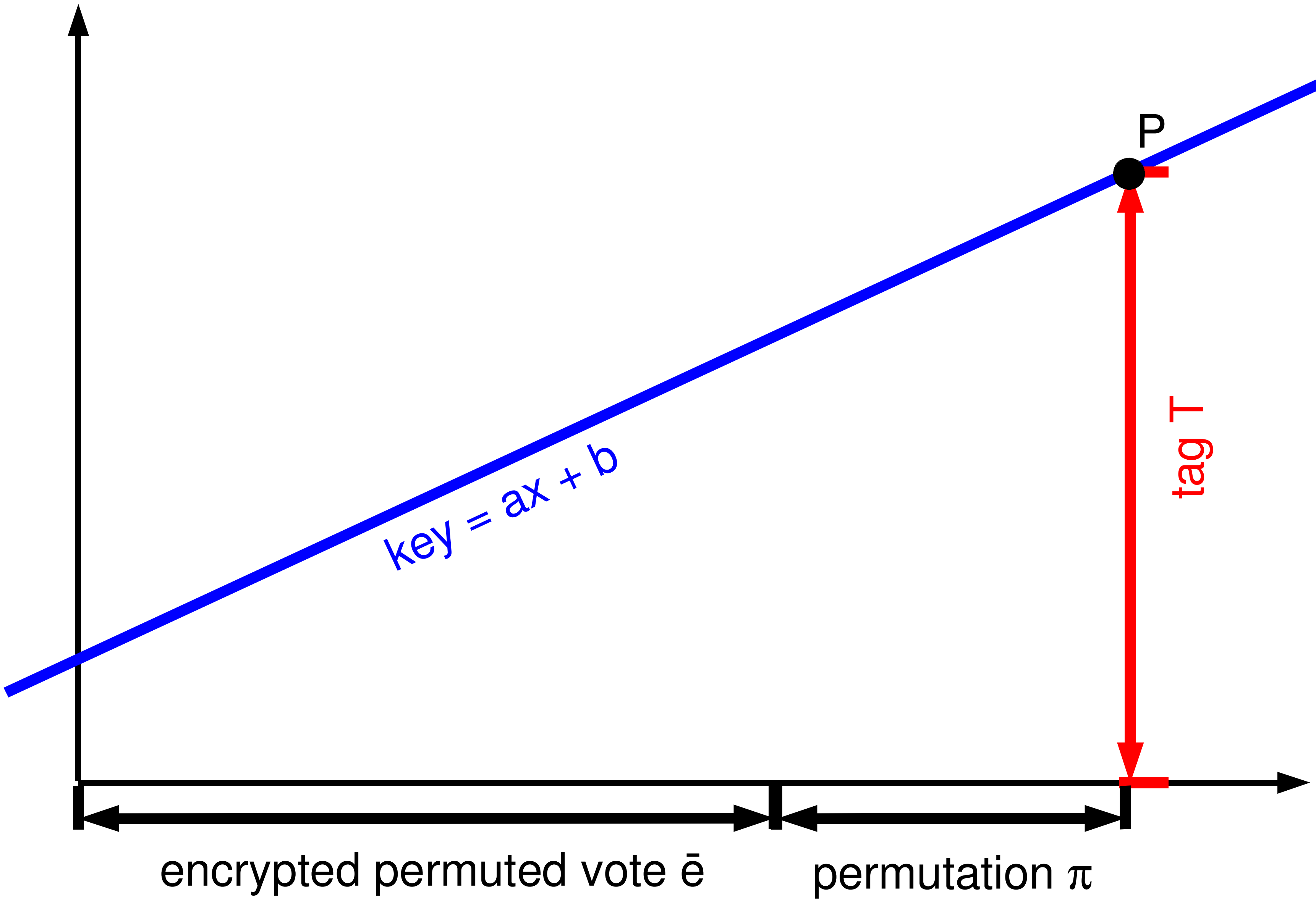
$$\begin{tikzcd}
v \arrow[d, "\text{homomorphic encryption}"'] & \text{casted vote} \\
e \arrow[d, "\text{blinding with correct key}"'] & \\
\bar{e} & \text{encrypted and blinded vote as sent in ballot} \\
e' \arrow[u, "\text{blinding with fake key}"] & \\
v' \arrow[u, "\text{homomorphic encryption}"] & \text{claimed vote}
\end{tikzcd}$$

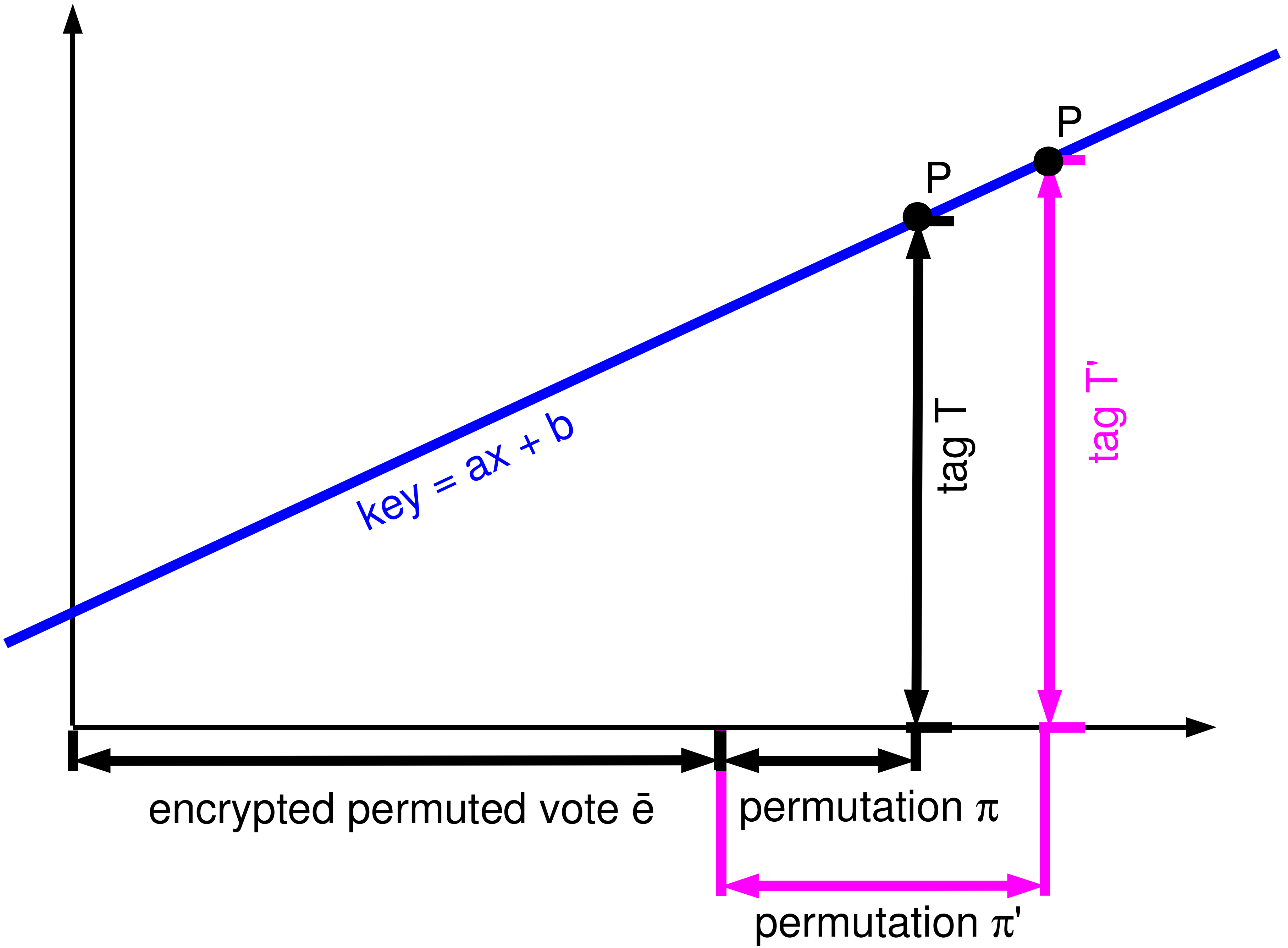

claimed vote
casted vote
v'
e'
ē
e
v
Cand 1
Cand 2
.....
Cand L
0 0 0 0 0 0 1
E(0) E(0) E(0) E(0) E(0) E(0) E(1)
E(0) E(0) E(0) E(0) E(0) E(1) E(0)
E(0) E(1) E(0) E(0) E(0) E(0) E(0)
0 1 0 0 0 0 0

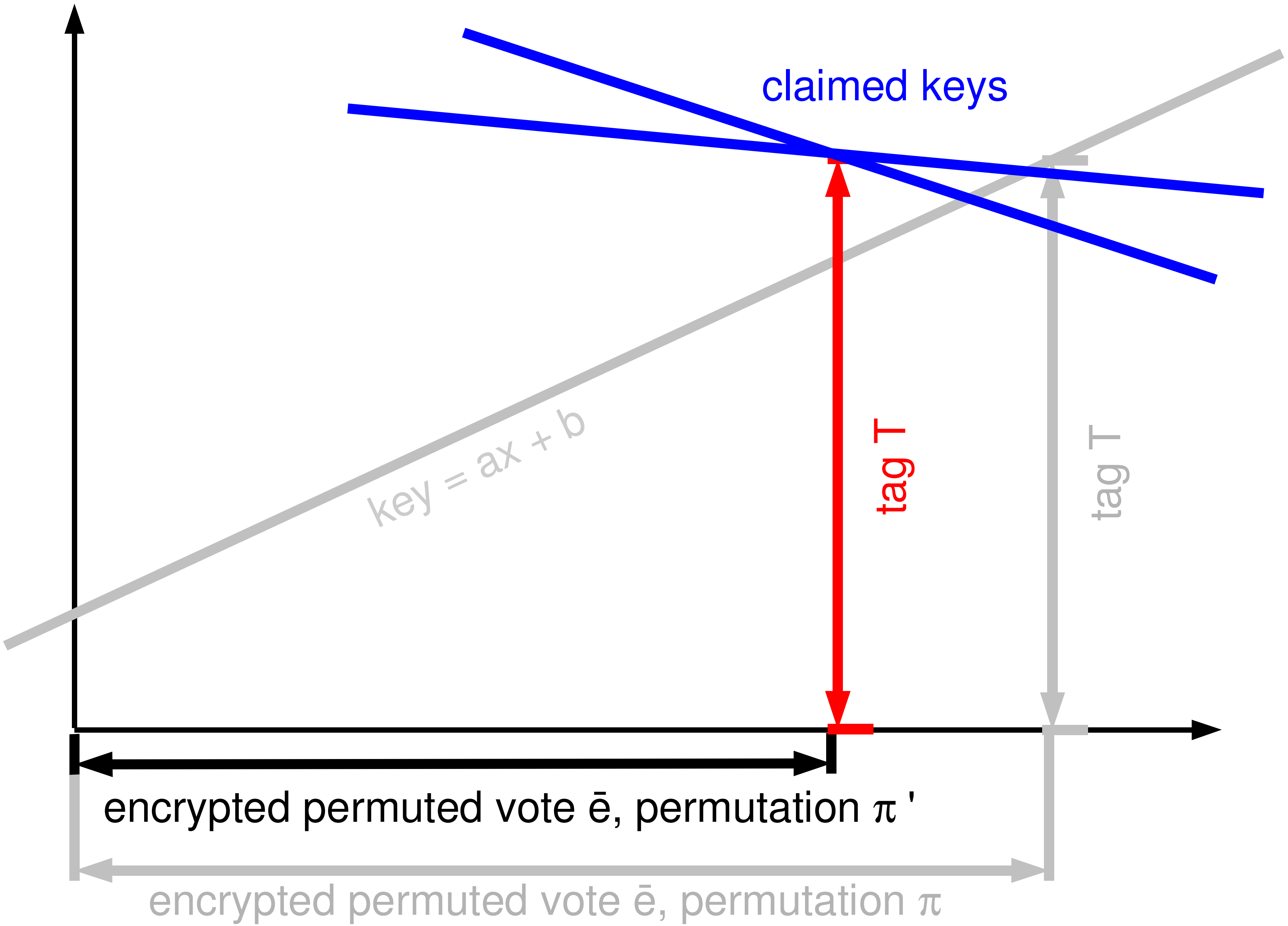




ballot = (voter ID,
vote ID,
encrypted and permuted vote $\bar{e}$,
validity proof,
tag,
signature)


P
key = ax + b
tag T
encrypted permuted vote ē
permutation π


P
P
key = ax + b
tag T
tag T'
encrypted permuted vote ē
permutation π
permutation π'


claimed keys
key = ax + b
tag T
tag T
encrypted permuted vote ē, permutation π '
encrypted permuted vote ē, permutation π

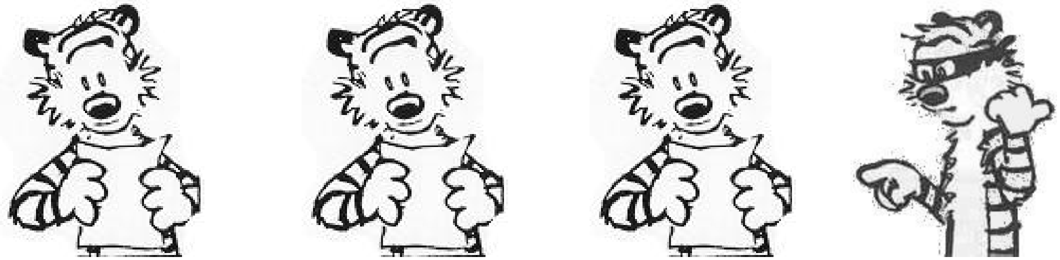
Possible States for each Voter

empty: No correctly signed ballot

invalid: One or more correctly signed but only invalid ones

valid: Exactly one correctly signed and valid

double: More than one correctly signed and valid ones



List of Accusations	I	II	I	~~IIII~~ I

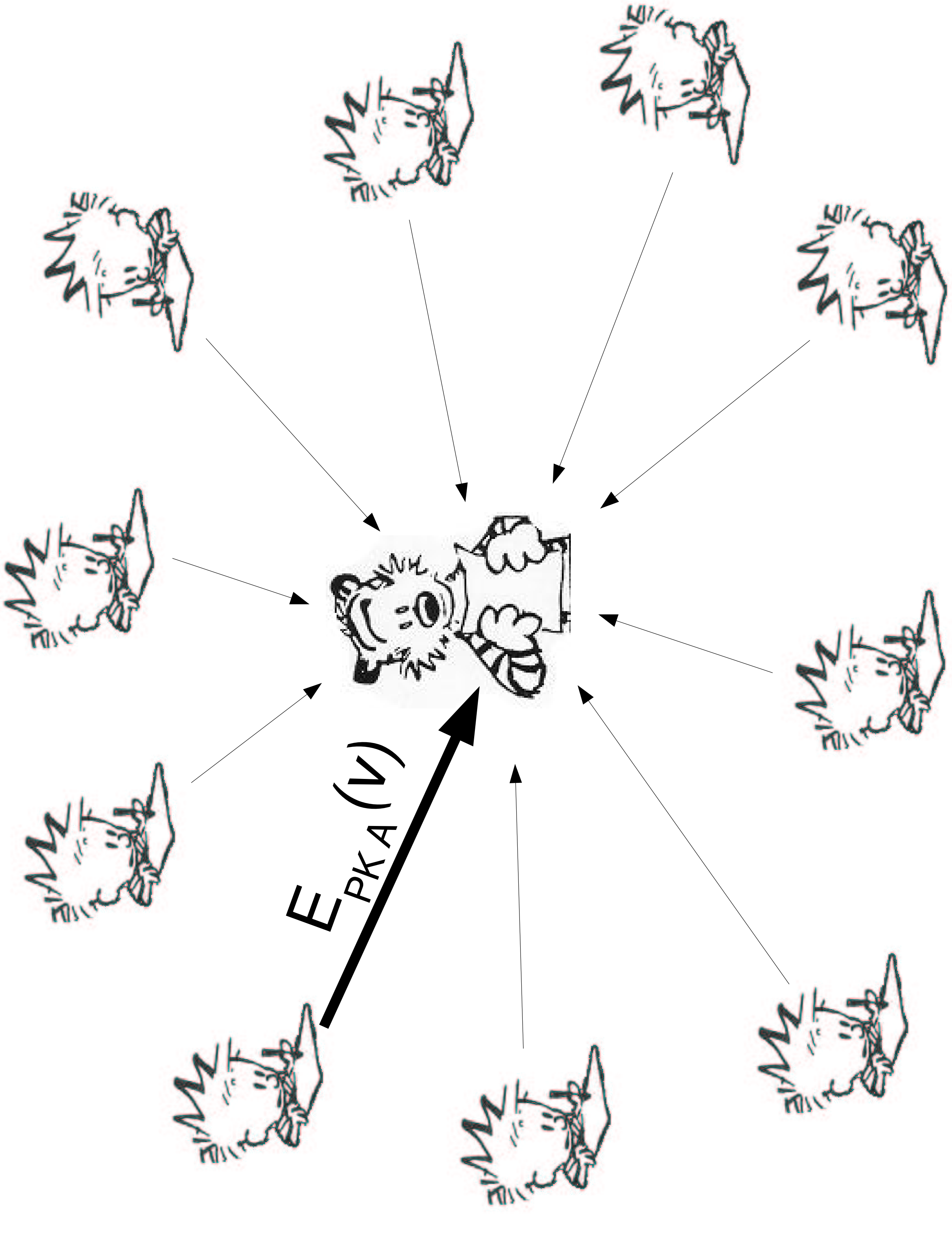
The Voter's View

- Receives letter with a permutation and a key
- Chooses his vote
- Encrypts his vote
- Permutes the encrypted vote
- Sends it to at least one honest authority
- Generates fake keys for each permutation he wants to claim
- “Proves” to the votebuyer that he has casted the desired vote

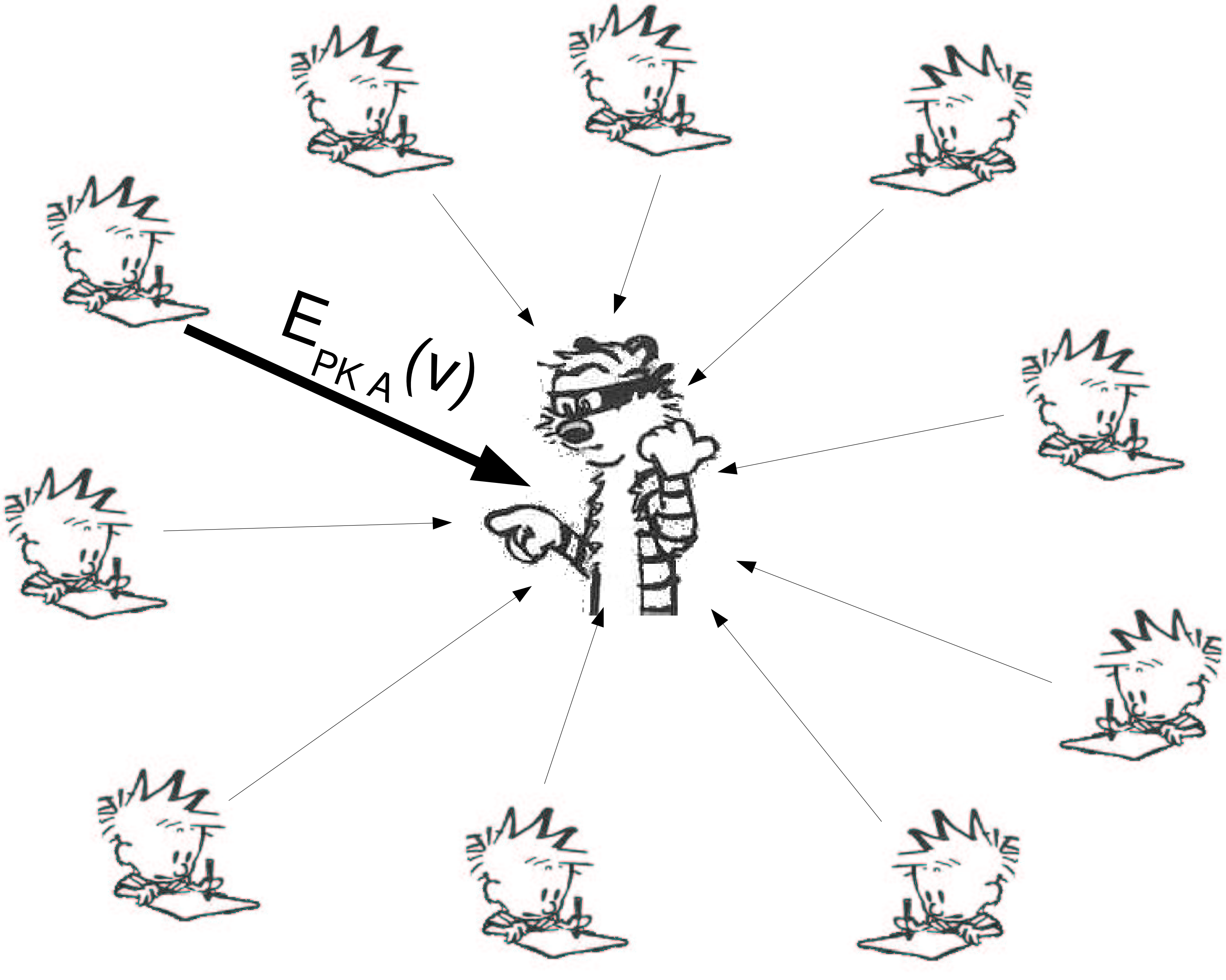
Properties of this Protocol

- Privacy: Yes!
- Availability: Yes!
- Correctness: Not completely,
  detection of irregularities
  but no prevention

- Receipt-freeness:
  Yes!



$E_{PK_A}(v)$



$E_{PK_A}(v)$

Vielen Dank für die Aufmerksamkeit!