KU LEUVEN

New Techniques for Electronic Voting

August 11, 2015

Alan Szepieniec and Bart Preneel
firstname.lastname@esat.kuleuven.be
KU Leuven, ESAT/COSIC and
iMinds, Belgium

Outline

0. UC Voting with Universal Verifiability
1. Tally-Hiding Vote
2. Self-Tallying Vote
3. Authenticated Voting Credentials

	UV	UC
THV	✓	✓
STV	✓	✓
AVC	✓	✓

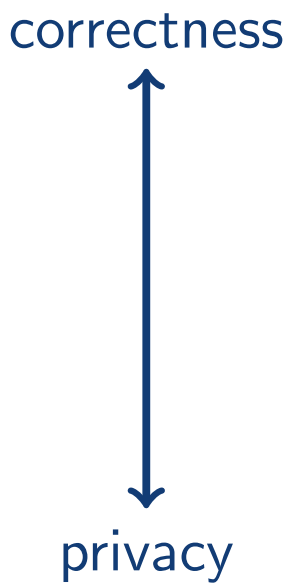
0. Universally Composable Voting

Voting System

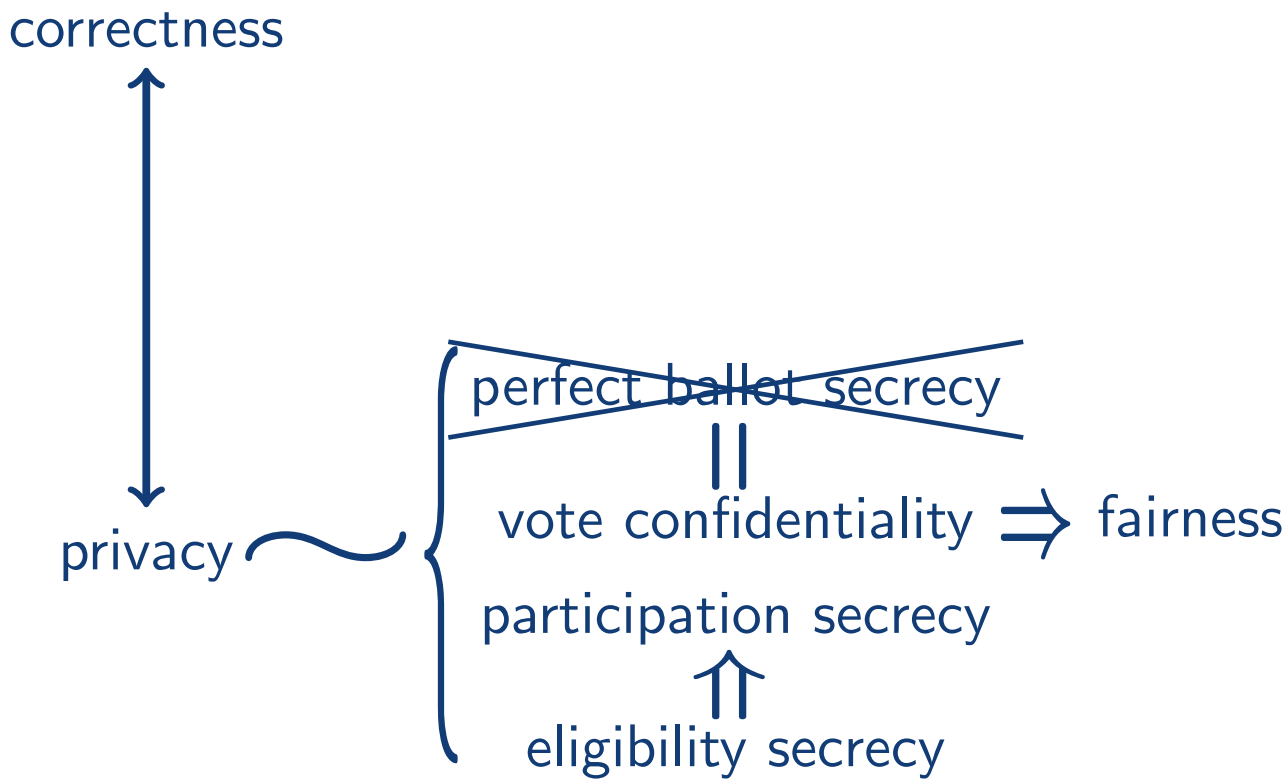
Definition

Let $\mathbf{O}$ be a set of *options* and $\mathrm{P}\mathbf{O}$ be the set of permutations of this set. Let $f : (\mathrm{P}\mathbf{O})^n \to \{0,1\}^*$ be a *tallying function*.
A *voting system* is an interactive protocol between *voters* $V_1, \ldots V_n$, who each hold a *vote* $v_i \in \mathrm{P}\mathbf{O}\, \forall i \in \{1, \ldots, n\}$, and *authorities* $A_1, \ldots, A_k$, if it computes the tally $t = f(v_1, \ldots, v_n)$.

Properties of Voting Systems

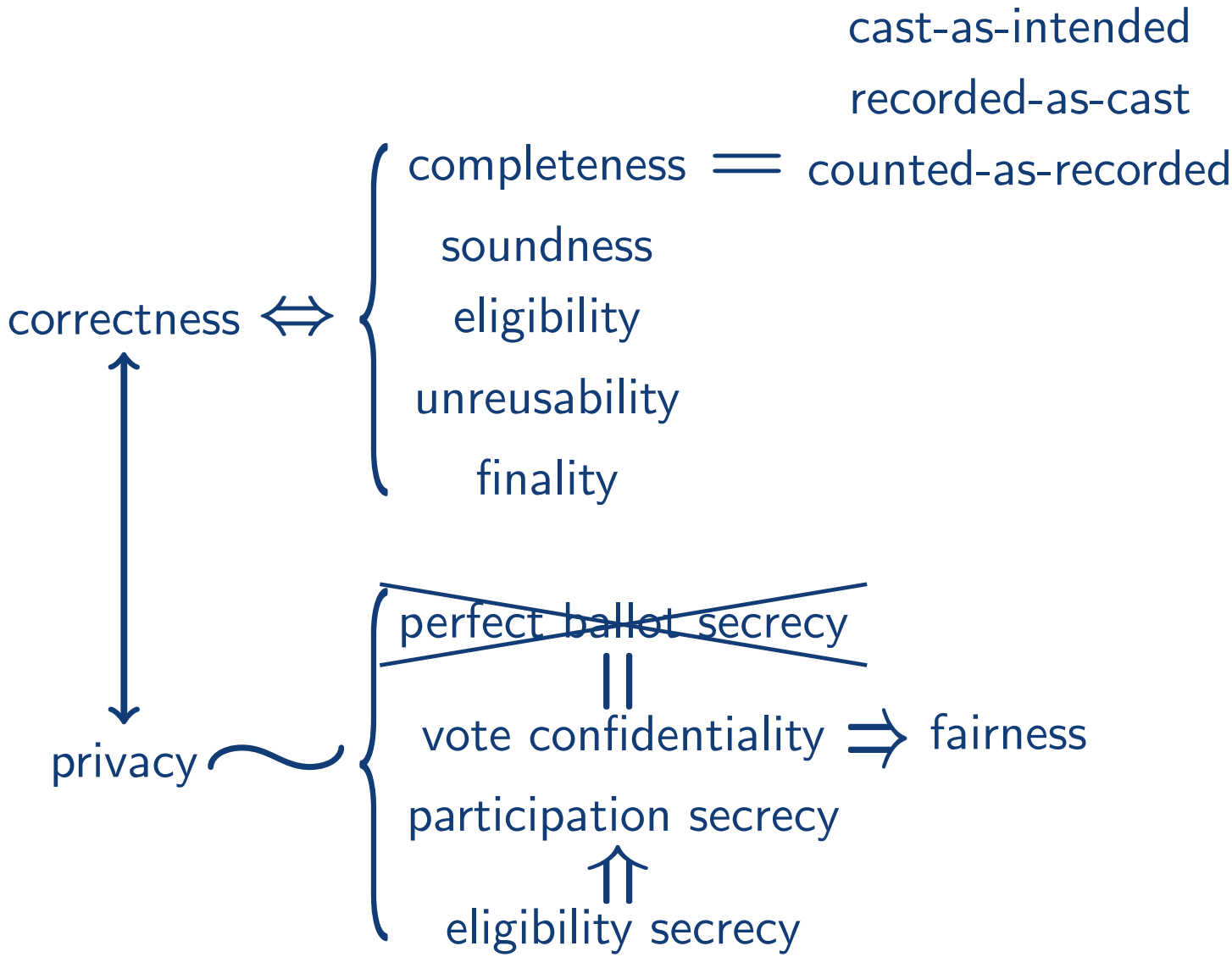


Properties of Voting Systems

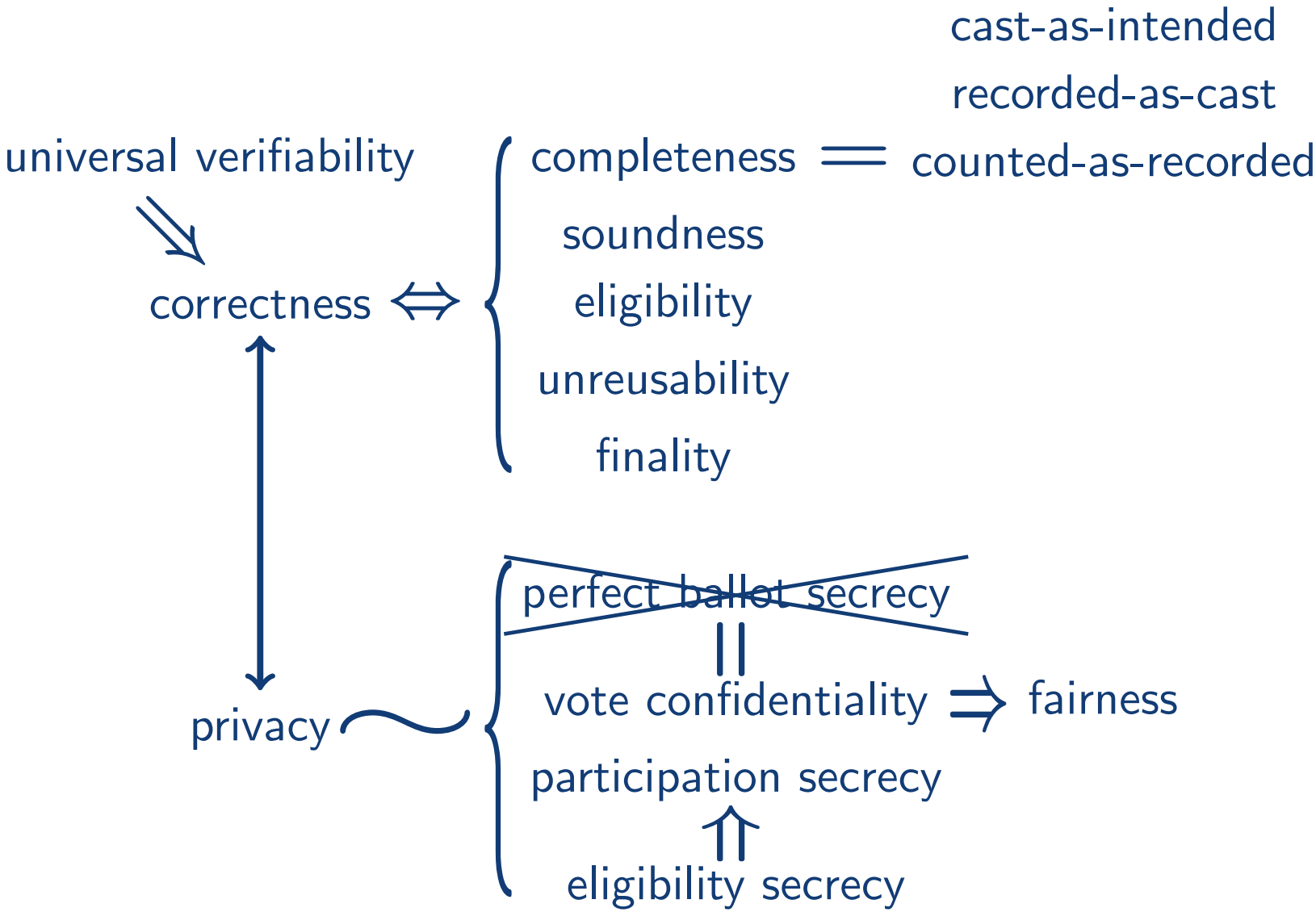


Properties of Voting Systems

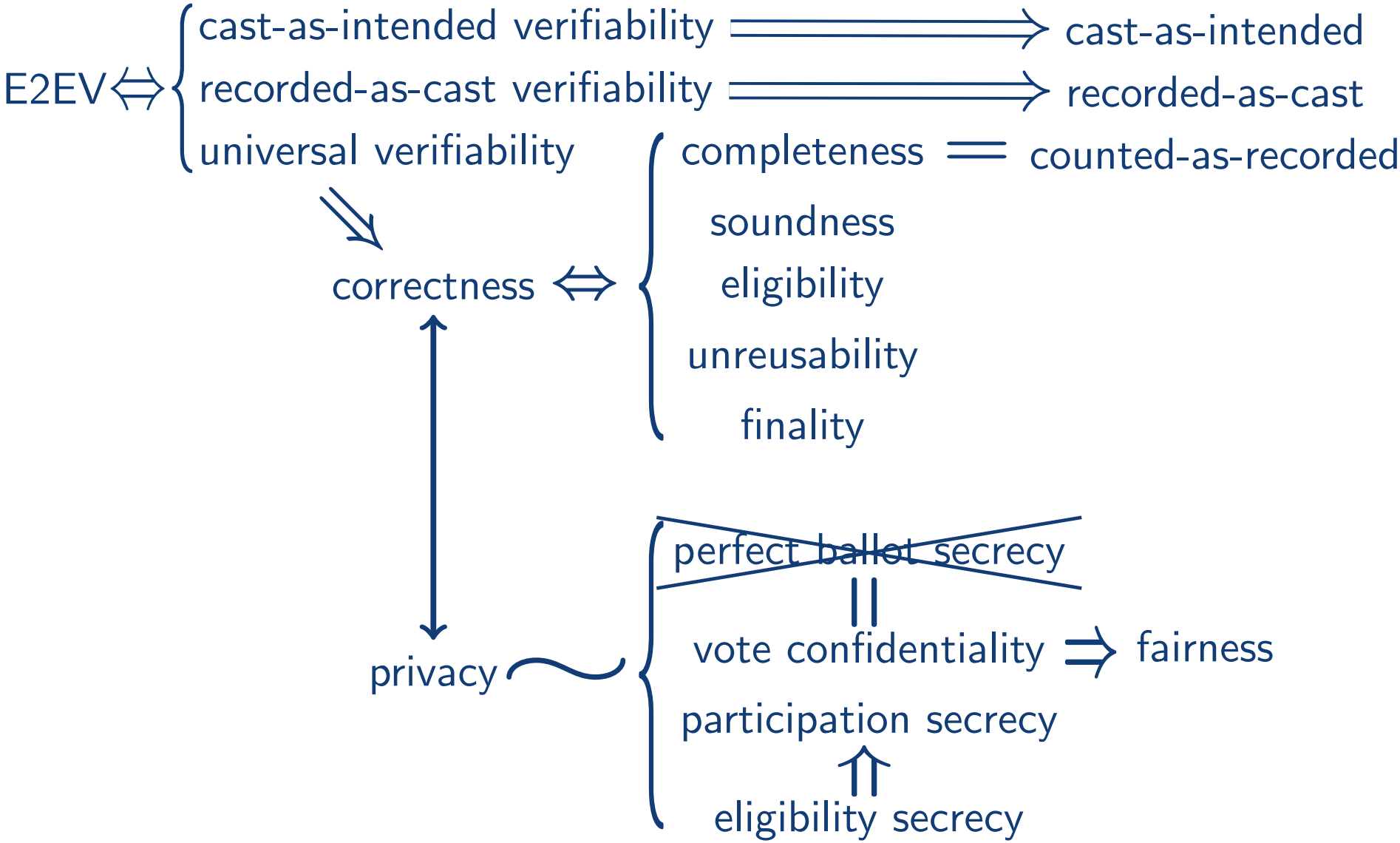
Properties of Voting Systems



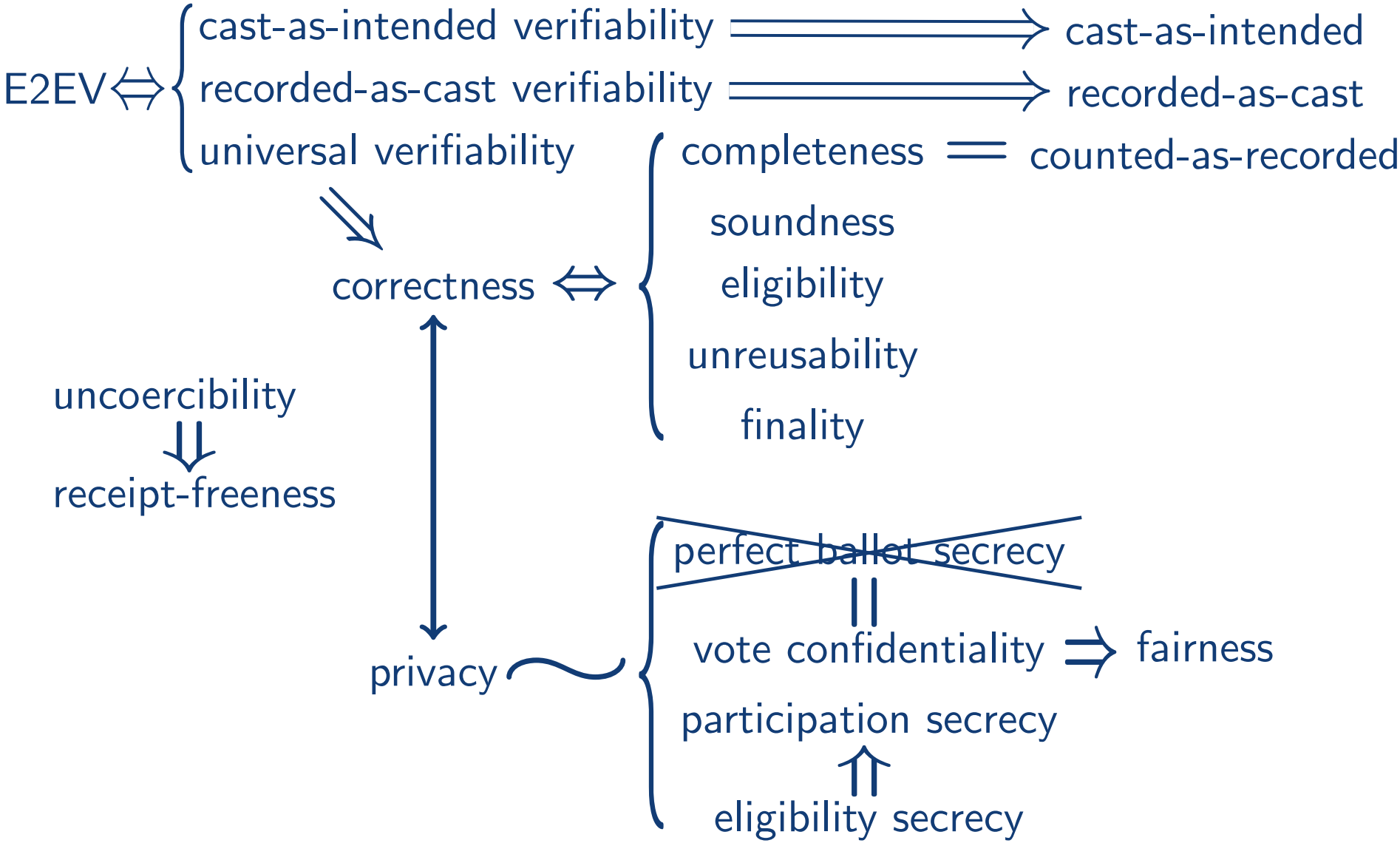
Properties of Voting Systems



Properties of Voting Systems



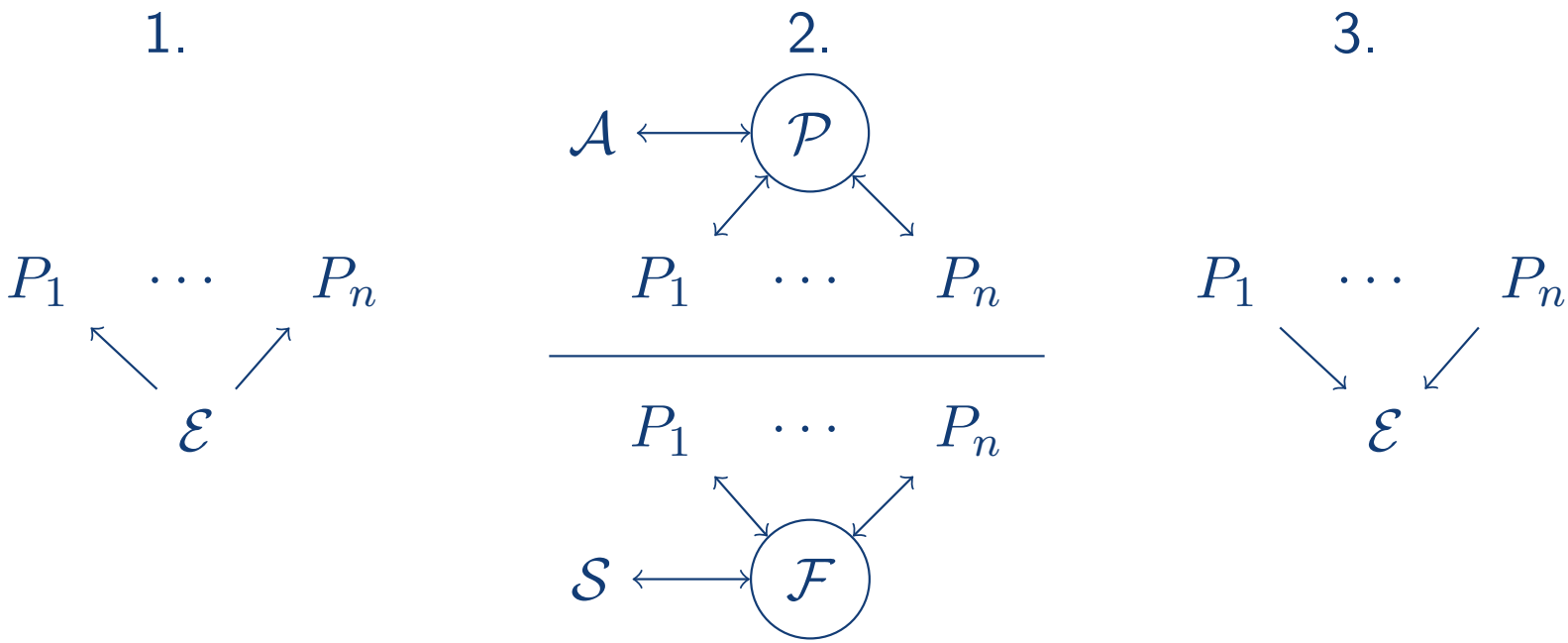
Properties of Voting Systems



Universal Composability

- standard framework for provable security of protocols
- composability $\Rightarrow$ allows modular protocol design
- ideal functionality $\mathcal{F}$: abstract description
- protocol $\mathcal{P}$: concrete instantiation of $\mathcal{F}$
- an experiment is conducted in one of two worlds:
  - *real world*: an adversary $\mathcal{A}$ attacks $\mathcal{P}$
  - *ideal world*: a simulator $\mathcal{S}$ attacks $\mathcal{F}$
- the *environment machine* $\mathcal{E}$:
  - chooses players' inputs beforehand;
  - reads players' outputs afterwards;
  - decides in which world the experiment took place

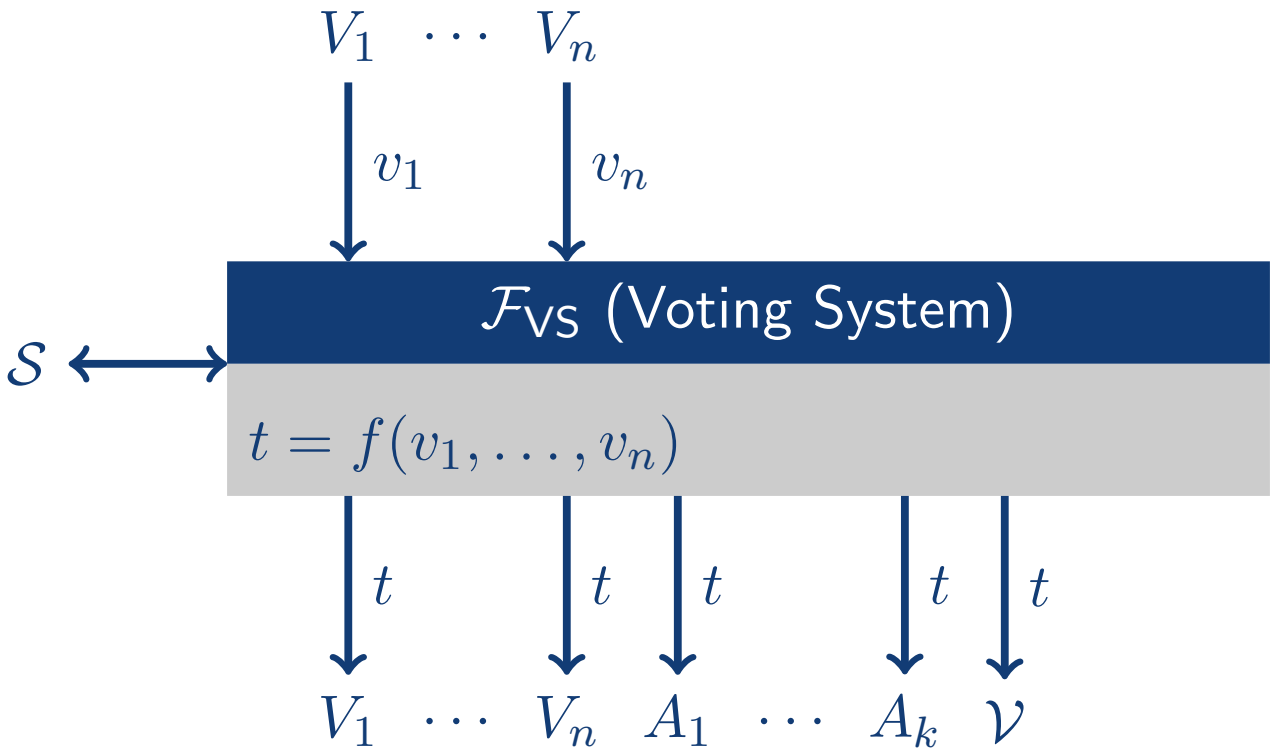
Universal Composability



Definition

Protocol $\mathcal{P}$ is a *UC-secure realization* of ideal functionality $\mathcal{F}$ if for all adversaries $\mathcal{A}$ attacking $\mathcal{P}$, there exists an adversary-simulator $\mathcal{S}$ attacking $\mathcal{F}$ such that no environment $\mathcal{E}$ can tell the difference.

Ideal Functionality: Voting System



- $\mathcal{S}$ can block votes
- $\mathcal{F}$ computes t *when the authorities say so*
- $\mathcal{V}$ receives t also

UC Voting System

$\mathcal{P}_{\mathsf{VS}}$ (Voting System)

$\mathcal{F}_{\mathsf{BB}}$

Bulletin Board: anonymous, public access append-only list of messages

$\mathcal{F}_{\mathsf{PKG}}$

Participant Key Gen: generates and distributes keypairs for each participant

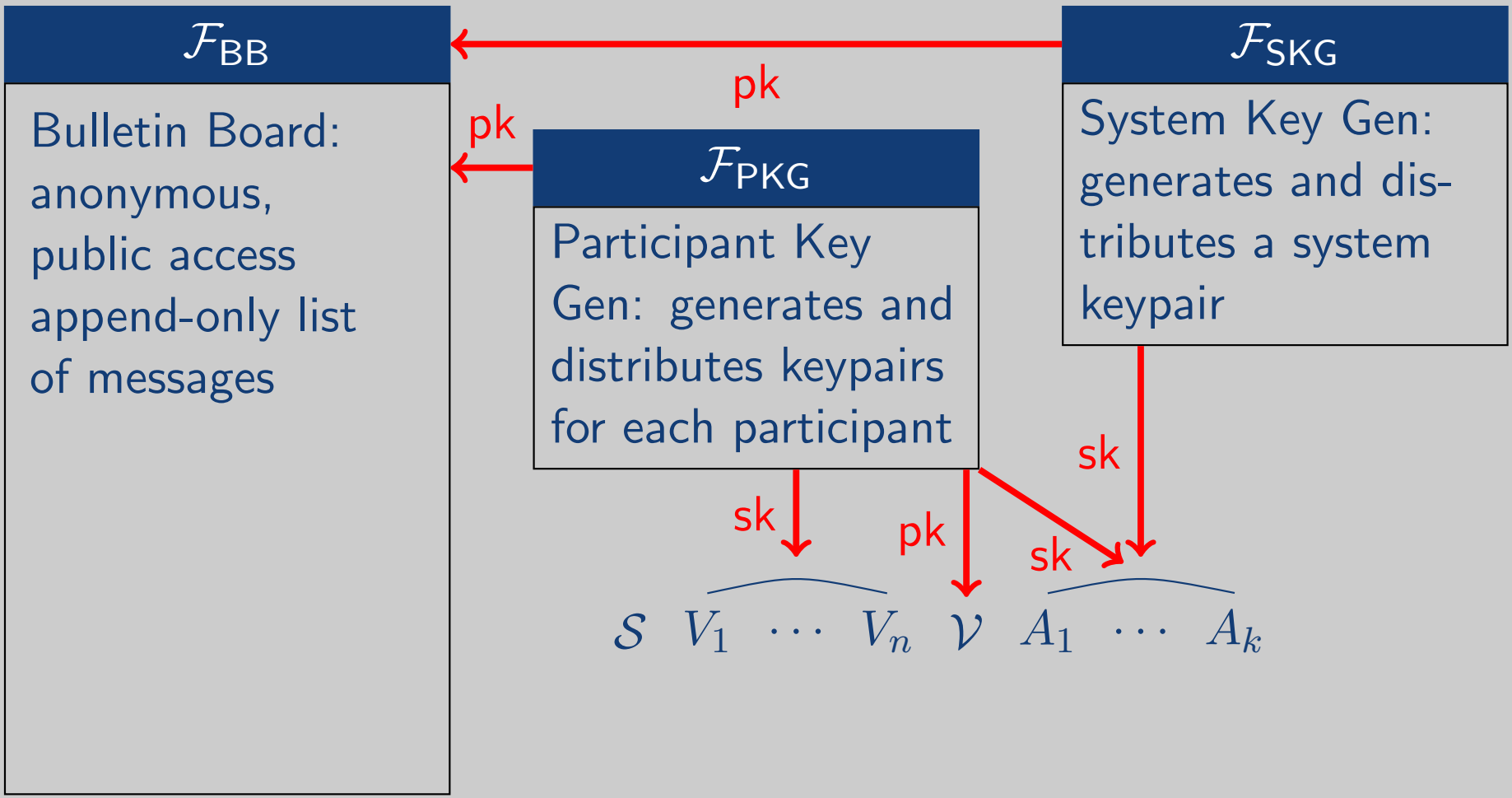
$\mathcal{F}_{\mathsf{SKG}}$

System Key Gen: generates and distributes a system keypair

$$\mathcal{S} \overbrace{V_1 \cdots V_n} \mathcal{V} \overbrace{A_1 \cdots A_k}$$

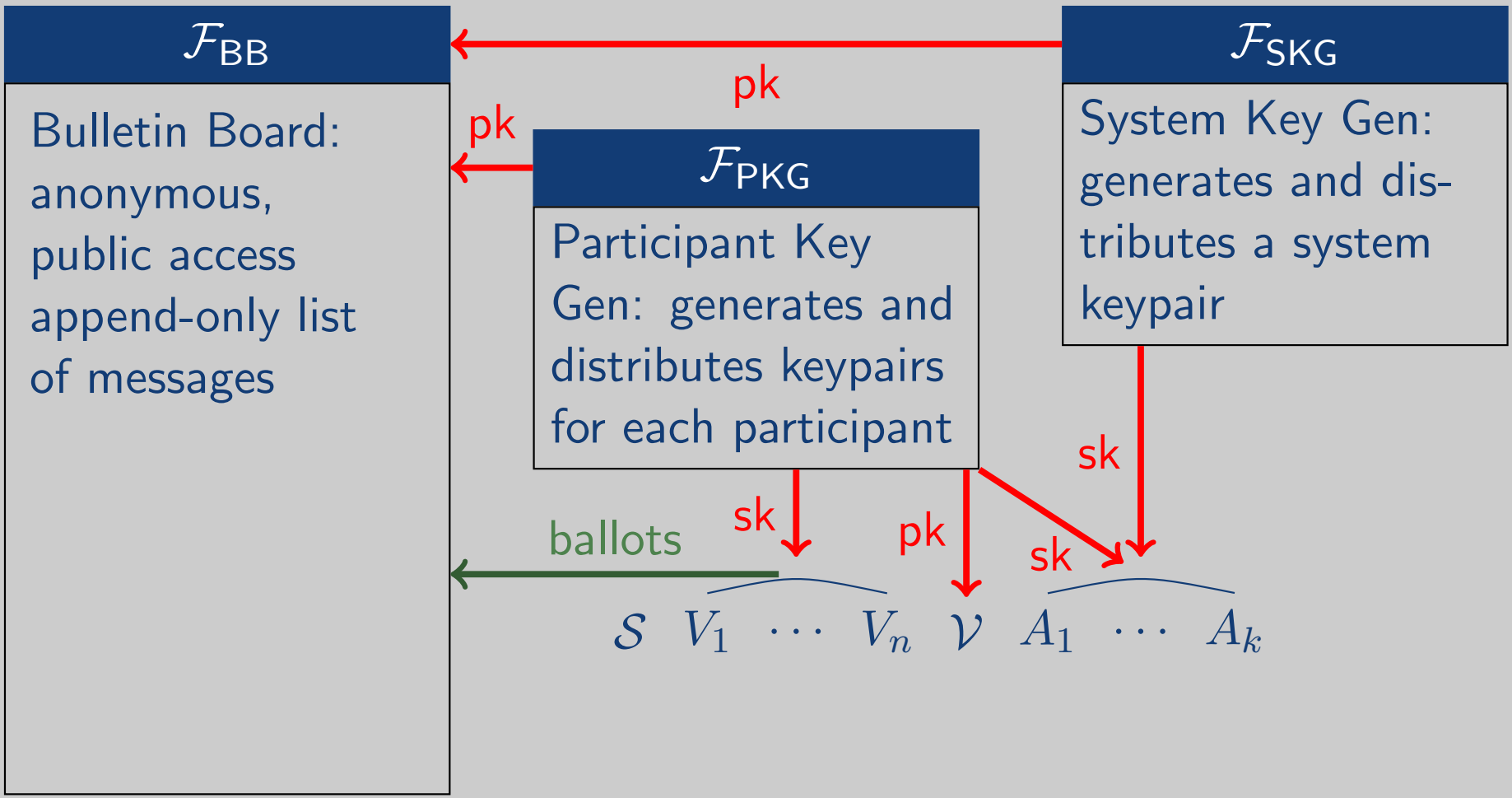
UC Voting System

$\mathcal{P}_{\mathsf{VS}}$ (Voting System)

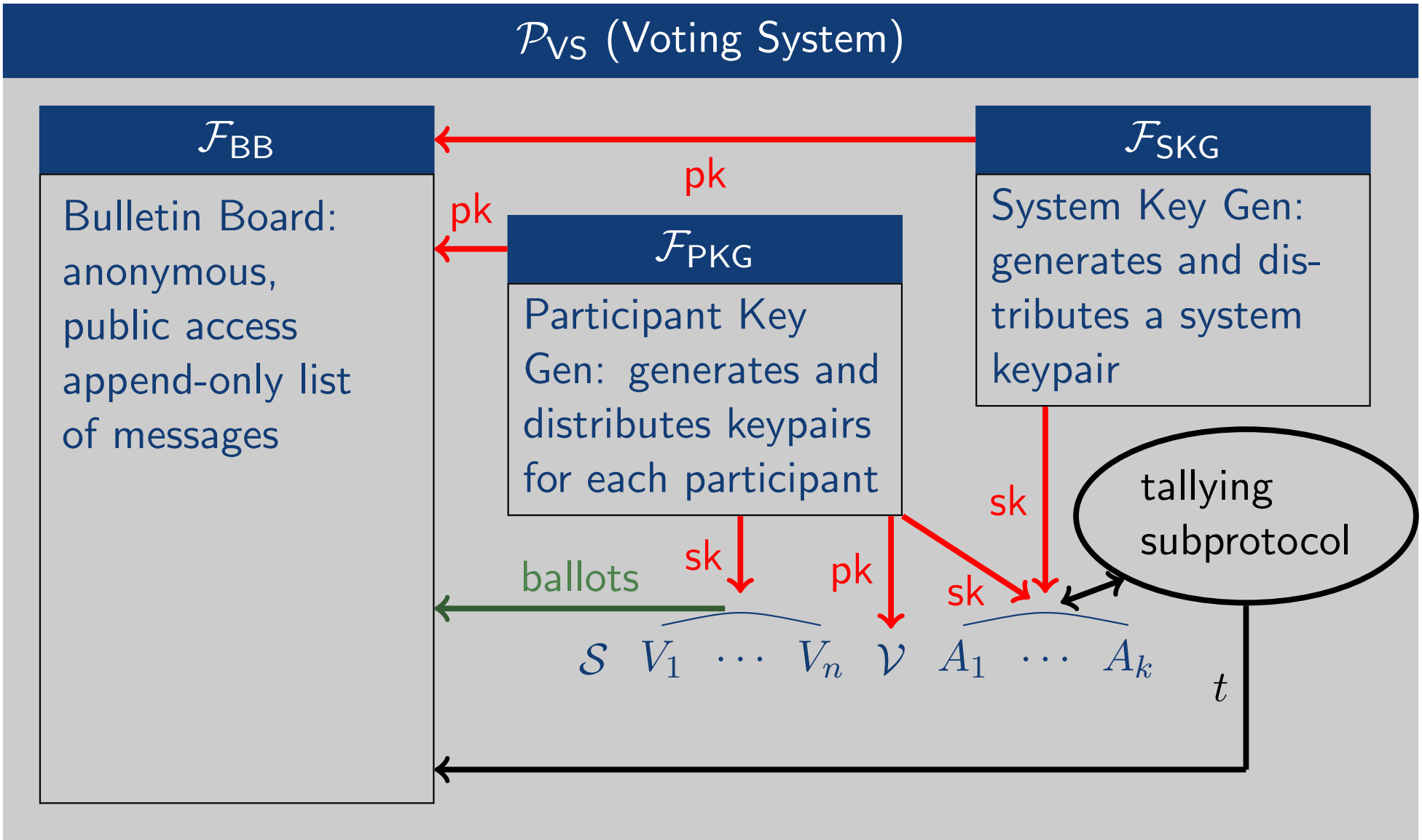


UC Voting System

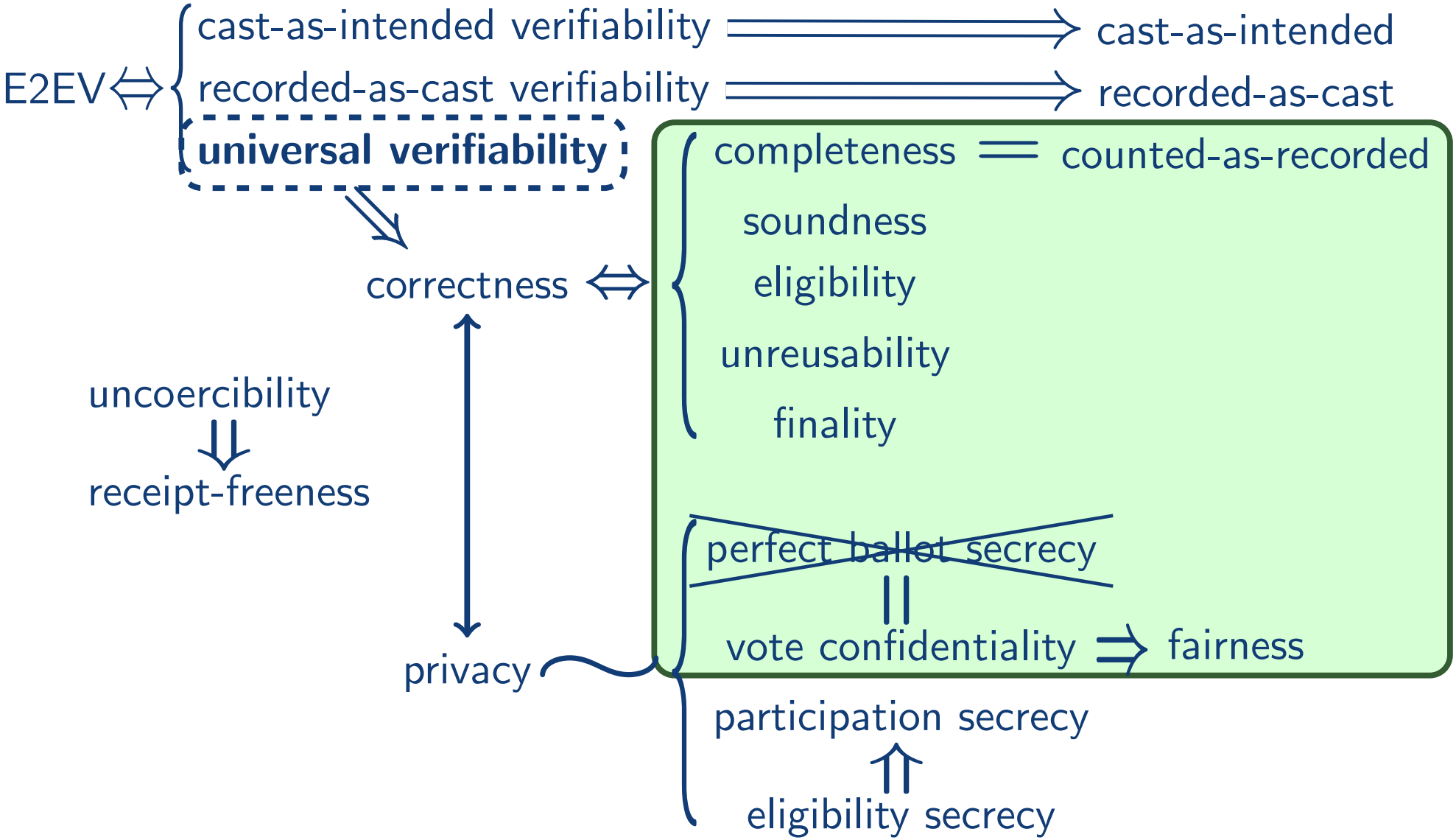
$\mathcal{P}_{\mathsf{VS}}$ (Voting System)



UC Voting System



Properties of UC-Secure Voting Systems



Universal Verifiability

1. 

2. 

3. 

Definition

Protocol $\mathcal{P}$ is *universally verifiable* if there exists a verifier $\mathcal{V}$ who retains, for all adversaries $\mathcal{A}$ attacking $\mathcal{P}$, significant distinguishing power:

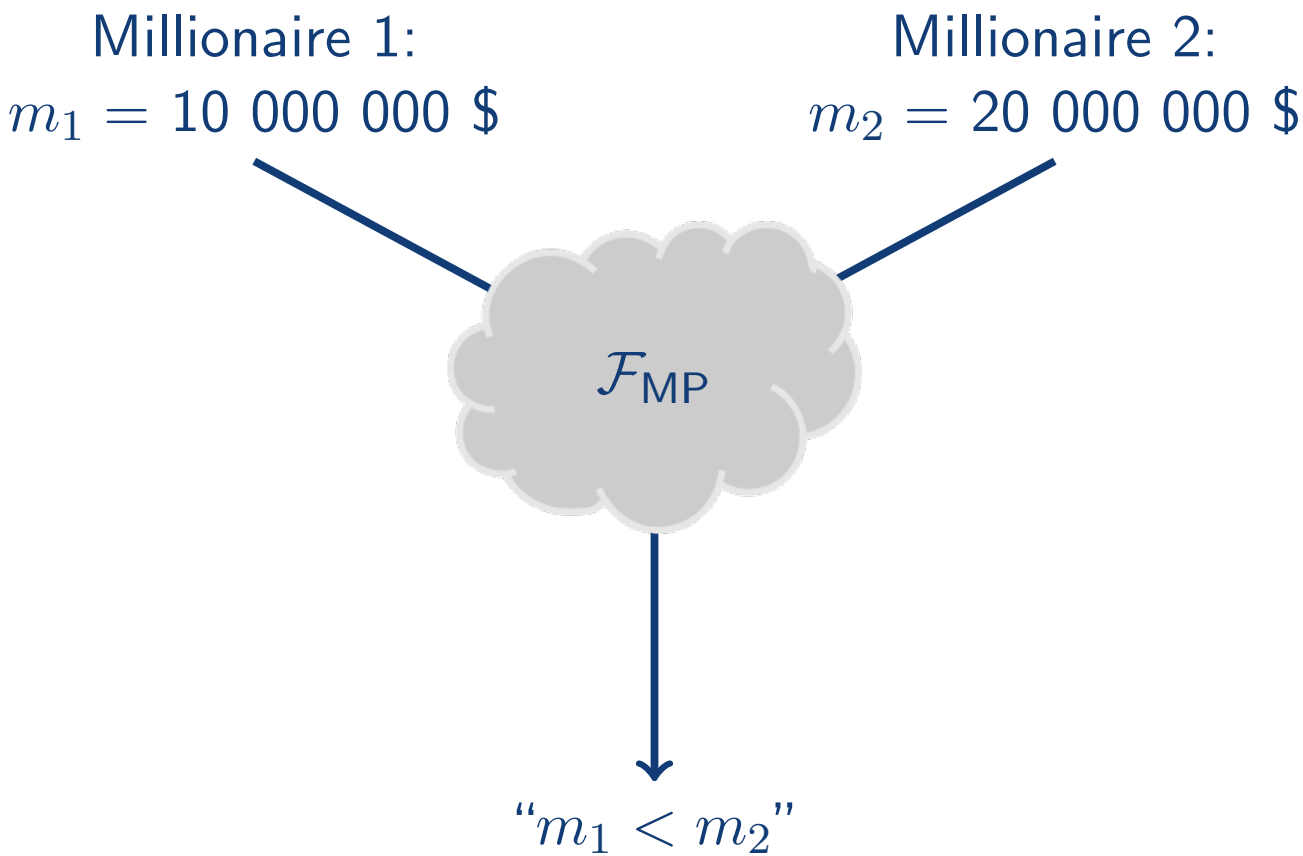
$$|\mathsf{Pr}[b = \hat{b}] - \mathsf{Pr}[b \neq \hat{b}]| \geq \frac{1}{2} \ .$$

1. Tally-Hiding Vote

Tally-Hiding Vote: Idea

- vote counts leak unnecessary information
- vote counts remain hidden
- tally identifies the winning option
- better name: *vote count hiding*
- preferential votes don't need vote counts

Millionaire Problem



UC-Secure Tally-Hiding Vote

two options: A and B

1. voters cast ballots: $\forall i : V_i \xrightarrow{\mathsf{E}(v_{i,A}), \mathsf{E}(v_{i,B})} \mathcal{F}_{\mathsf{BB}}$
2. homomorphic aggregation: $\mathsf{E}(c_A) = \mathsf{E}(\sum_i v_{i,A})$ and $\mathsf{E}(c_B)$
3. millionaire problem: $t = \mathcal{F}_{\mathsf{MP}}(\mathsf{E}(c_A), \mathsf{E}(c_B))$

Paillier Cryptosystem

KeyGen(1^κ):

$p, q \xleftarrow{\$}$ random primes

$n \leftarrow pq$ (public key)

$d = 1 \mod n$ and

$d = 0 \mod \varphi(n)$ (private key)

Encrypt(m):

$r \xleftarrow{\$} \mathbb{Z}_{n^2}$

$\mathsf{E}(m) = (1+n)^m r^n \mod n^2$

Decrypt(c):

$\ell \leftarrow c^d \mod n^2$

$m \leftarrow \frac{\ell - 1}{n}$

Homomorphic Add(c_1, c_2):

$c \leftarrow c_1 c_2 \mod n^2$

Millionaire Problem Protocol for Paillier

Damgård-Jurik cryptosystem:

$$\mathsf{E}_2(m) = (1+n)^m r^n \mod n^3 \qquad m \in \mathbb{Z}_{n^2}$$

Black-box lifting procedure Lift maps a Paillier ciphertext ($m \in \mathbb{Z}_n$) to a Damgård-Jurik ciphertext ($m \in \mathbb{Z}_{n^2}$).

$$\mathsf{Lift} : \mathbb{Z}_{n^2} \to \mathbb{Z}_{n^3}$$

Millionaire Problem (c_1, c_2):

$B \leftarrow \mathsf{Lift}(c_1) \ominus \mathsf{Lift}(c_2)$

$A \leftarrow \mathsf{Lift}(c_1 \ominus c_2)$

$\mathsf{D}(B \ominus A) = 0 \Rightarrow$ no overflow $\Rightarrow c_1 \geq c_2$

$\mathsf{D}(B \ominus A) \neq 0 \Rightarrow$ overflow! $\Rightarrow c_1 < c_2$

Ciphertext Lifting

secret key is distributed among authorities $A_1, \ldots, A_k$ s.t.

$$(1+n)^{4\Delta^2 m} = 1 + 4\Delta^2 mn = \prod_i c^{4\Delta^2 s_i \prod_{j\neq i} \frac{-j}{i-j}} \mod n^2 \ .$$

Lift(c) :

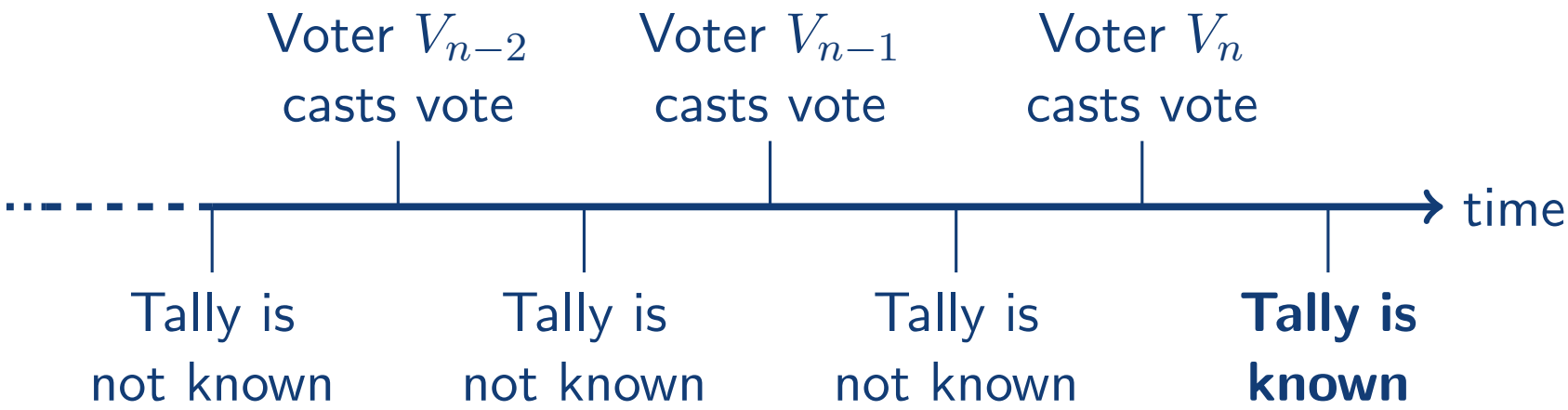
- $1 + 4\Delta^2 \underline{m} n = \prod_i \underline{c_i} \mod n^2$
- $\underline{c_i}^{(4\Delta^2)^{-1} \mod n} = a_i + n\underline{b_i} \mod n^2$ with $a_i < n$
- $\underline{m} = \left[\prod_i a_i\right]_2 + \sum_i \underline{b_i} \prod_{j\neq i} a_j \mod n^*$
- $\mathsf{E}_2(\underline{m}) =$
  $\mathsf{E}_2\left(\left[\prod_i a_i\right]_2\right) \oplus \mathsf{E}_2\left(\underline{b_1} \prod_{j\neq 1} a_i\right) \oplus \mathsf{E}_2\left(\underline{b_2} \prod_{j\neq 2} a_i\right) \oplus \cdots$

2. Self-Tallying Vote

Self-Tallying Vote: Idea

- cut out the expensive tallying procedure
- tally is known as soon as last vote is cast (but not before)

Control Voter



- V_n knows the tally *before casting his vote*
- violates *fairness*
- cannot be UC-secure
- solution: V_n *cannot be corrupted*

Self-Tallying Vote with Paillier

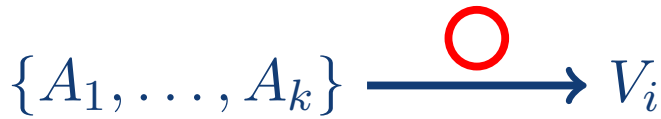
- $\mathcal{F}_{\mathsf{SKG}}$ distributes x_i among voters s.t. $\sum_i x_i = 0$
- common randomizer $r \in \mathbb{Z}_{n^2}$ (from timestamp or hash)
- voters encrypt votes as $c_i = (1+n)^{v_i} r^{x_i n} \mod n^2$
- homomorphic aggregation:

$$
\begin{aligned}
1 + nt &= c_1 \oplus c_2 \oplus \cdots \oplus c_n \\
&= \prod_i c_i \mod n^2 \\
&= \prod_i (1+n)^{v_i} r^{n x_i} \mod n^2 \\
&= \left(\prod_i (1+n)^{v_i} \right) (r^n)^{\sum_i x_i} \mod n^2 \\
&= \prod_i (1+n)^{v_i} \mod n^2 \\
&= 1 + n \sum_i v_i \mod n^2
\end{aligned}
$$

3. Authenticated Voting Credentials

Voting Credentials: Idea

initialization:



voting:

tallying:

$$t = \sum_i v_i$$

- *anonymous access* to $\mathcal{F}_{\mathsf{BB}}$
- fairness $\Rightarrow$ $\mathcal{A}$ *cannot read* $\mathcal{F}_{\mathsf{BB}}$ *during voting*
- invalid credential $\Rightarrow$ v_i not counted
- duplicate credential $\Rightarrow$ v_i not counted

Authenticated Voting Credentials

adversarial model:

authenticated voting credential:

- $\mathcal{A}$'s vote does not match credential $\Rightarrow$ invalid ballot
- the credential is authenticated by the vote
- *the credential cannot be re-purposed*

Ferguson Credential Withdrawal

Public knowledge: n, v, g, h.
Private knowledge for $\mathcal{B}$: $1/v = v^{-1} \mod \varphi(n)$.

$\mathcal{A}$		$\mathcal{B}$
$a_1, \gamma, \sigma \xleftarrow{\$} \mathbb{Z}_n^*$		
$b \leftarrow \gamma^v a_1 g^\sigma \mod n$		
$a_2 \leftarrow \mathsf{H}(b)$		
$a \leftarrow a_1 a_2 \mod n$		
$c \leftarrow f(h^a) - \sigma$		
	$\xrightarrow{b, c}$	
		$a_2 \leftarrow \mathsf{H}(b)$
		$\bar{A} \leftarrow (b a_2 g^c)^{1/v} \mod n$
	$\xleftarrow{\bar{A}}$	
$S \leftarrow \bar{A}\gamma^{-1} \mod n$		

- credential: (S, a) such that $S^v = a g^{f(h^a)} \mod n$
- $\mathcal{B}$ learns no information on S or a

Guillou-Quisquater Proof

Public knowledge: n, v, A.
Private knowledge for $\mathcal{P}$: S s.t. $S^v = A \mod n$.

$\mathcal{P}$		$\mathcal{V}$
$d \xleftarrow{\$} \mathbb{Z}_n^*$		
$D \leftarrow d^v \mod n$		
	$\xrightarrow{D}$	
		$e \xleftarrow{\$} \{0,1\}^{\lvert n \rvert}$
	$\xleftarrow{e}$	
$f \leftarrow dS^e \mod n$		
	$\xrightarrow{f}$	
		$f^v \stackrel{?}{=} A^e D \mod n$

- S is kept secret
- spent credential: (a, D, e, f)
- where $e = \mathsf{H}(A \parallel D \parallel v_i)$

Conclusion

- voting formalism
- universal composability + voting
- formalism of universal verifiability
- Tally-Hiding Vote
  - Millionaire Problem
  - Ciphertext Lifting
- Self-Tallying Vote
- Authenticated Voting Credentials

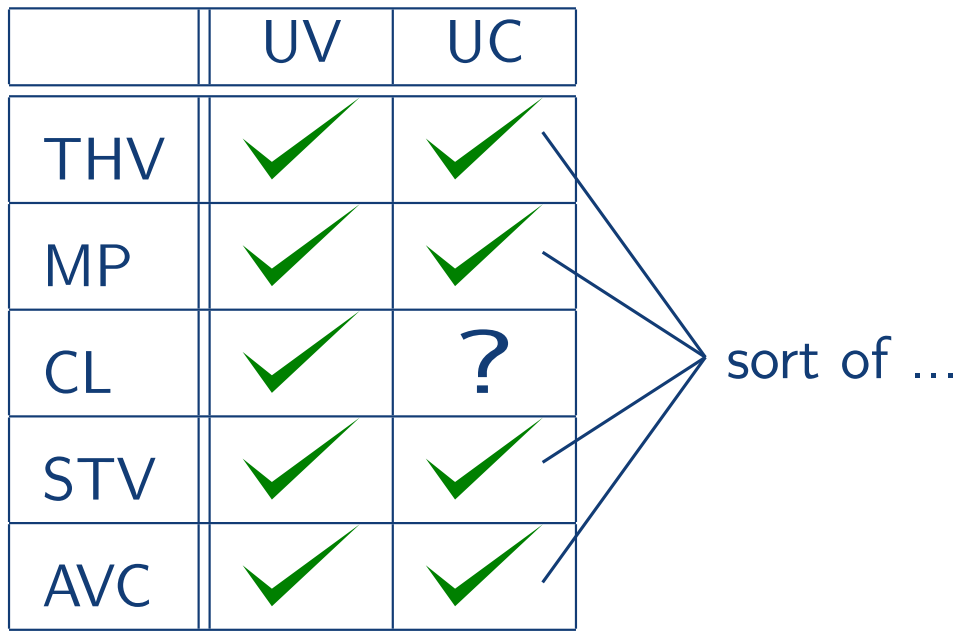
Conclusion

- voting formalism
- universal composability + voting
- formalism of universal verifiability
- Tally-Hiding Vote
  - Millionaire Problem
  - Ciphertext Lifting
- Self-Tallying Vote
- Authenticated Voting Credentials

	UV	UC
THV	✓	✓
MP	✓	✓
CL	✓	?
STV	✓	✓
AVC	✓	✓

Conclusion

- voting formalism
- universal composability + voting
- formalism of universal verifiability
- Tally-Hiding Vote
  - Millionaire Problem
  - Ciphertext Lifting
- Self-Tallying Vote
- Authenticated Voting Credentials



Conclusion

- voting formalism
- universal composability + voting
- formalism of universal verifiability

} future work: cover all properties

- Tally-Hiding Vote
  - Millionaire Problem
  - Ciphertext Lifting
- Self-Tallying Vote
- Authenticated Voting Credentials