Defining Privacy for Weighted Votes, Single and Multi-Voter Coercion

Jannik Dreier, Pascal Lafourcade, Yassine Lakhnech

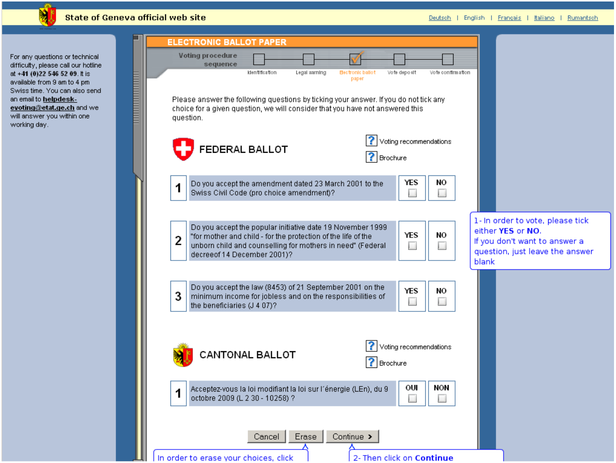
Université Grenoble 1, CNRS, Verimag, France

European Symposium on Research in Computer Security (ESORICS), Pisa, Italy
September 11, 2012

Internet voting

Available in

- Estonia
- France
- Switzerland
- ...



Security Requirements

Fairness

Verifiability

Eligibility

Correctness

Security Requirements

Privacy

Receipt-Freeness

Robustness

Coercion-Resistance

Security Requirements

Fairness

Verifiability

Eligibility

Correctness

Security Requirements

Privacy

Receipt-Freeness

Robustness

Coercion-Resistance

Defining Vote-Privacy [Swap-Privacy (SwP)]

Classical definition (e.g. [?, ?, ?]): Observational equivalence between two situations where two voters swap votes.

	Alice	Bob
Vote	A	B
	$\approx_l$	
Vote	B	A

Problem: Weighted Votes

What happens if votes are weighted (e.g. according to the number of shares in a company)?

	Alice	Bob	Result
	66%	34%	
Vote	A	B	
	$\approx_l$		
Vote	B	A	

Problem: Weighted Votes

What happens if votes are weighted (e.g. according to the number of shares in a company)?

	Alice	Bob	Result
	66%	34%	
Vote	A	B	66% A, 34% B

$$\approx_l$$

Vote	B	A	34% A, 66% B

Problem: Weighted Votes

What happens if votes are weighted (e.g. according to the number of shares in a company)?

	Alice	Bob	Result
	66%	34%	
Vote	A	B	66% A, 34% B
	$\approx_l$		$\neq$
Vote	B	A	34% A, 66% B

Problem: Weighted Votes

What happens if votes are weighted (e.g. according to the number of shares in a company)?

	Alice 66%	Bob 34%	Result
Vote	A	B	66% A, 34% B
	$\not\approx_l$		$\neq$
Vote	B	A	34% A, 66% B

Problem: Weighted Votes

Still: Some privacy is possible!

	Alice	Bob	Carol	Result
	50%	25%	25%	
Vote	A	B	B	
Vote	B	A	A	

Problem: Weighted Votes

Still: Some privacy is possible!

	Alice 50%	Bob 25%	Carol 25%	Result
Vote	A	B	B	50% A, 50% B
Vote	B	A	A	50% A, 50% B

Problem: Weighted Votes

Still: Some privacy is possible!

	Alice	Bob	Carol	Result
	50%	25%	25%	
Vote	A	B	B	50% A, 50% B
				=
Vote	B	A	A	50% A, 50% B

Problem: Weighted Votes

Still: Some privacy is possible!

	Alice	Bob	Carol	Result
	50%	25%	25%	
Vote	A	B	B	50% A, 50% B
		$\approx_l$		=
Vote	B	A	A	50% A, 50% B

Plan

Plan

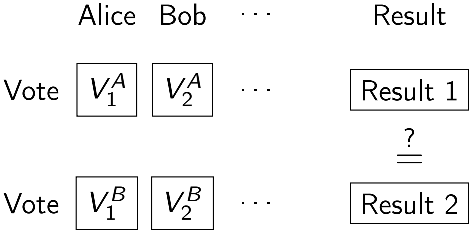
Solution: Defining Vote-Privacy (VP) for weighted votes

Idea: If two instances give the same result, they should be bisimilar.

	Alice	Bob	···	Result
Vote	V_1^A	V_2^A	···	Result 1
Vote	V_1^B	V_2^B	···	Result 2

Solution: Defining Vote-Privacy (VP) for weighted votes

Idea: If two instances give the same result, they should be bisimilar.



Solution: Defining Vote-Privacy (VP) for weighted votes

Idea: If two instances give the same result, they should be bisimilar.

	Alice	Bob	···		Result
Vote	V_1^A	V_2^A	···		Result 1
				$\Leftarrow$	$\stackrel{?}{=}$
Vote	V_1^B	V_2^B	···		Result 2

Solution: Defining Vote-Privacy (VP) for weighted votes

Idea: If two instances give the same result, they should be bisimilar.

	Alice	Bob	⋯		Result
Vote	V_1^A	V_2^A	⋯		Result 1
		$\approx_l$		$\Leftarrow$	$\stackrel{?}{=}$
Vote	V_1^B	V_2^B	⋯		Result 2

Example revisited

Applying the definition:

	Alice	Bob	Carol	Result
	50%	25%	25%	
Vote	A	B	B	50% A, 50% B
Vote	B	A	A	50% A, 50% B

Example revisited

Applying the definition:

	Alice 50%	Bob 25%	Carol 25%	Result
Vote	A	B	B	50% A, 50% B
				$\stackrel{?}{=}$
Vote	B	A	A	50% A, 50% B

Example revisited

Applying the definition:

	Alice	Bob	Carol	Result
	50%	25%	25%	
Vote	A	B	B	50% A, 50% B
			$\Leftarrow$	$\stackrel{?}{=}$
Vote	B	A	A	50% A, 50% B

Example revisited

Applying the definition:

	Alice	Bob	Carol	Result
	50%	25%	25%	
Vote	A	B	B	50% A, 50% B
		$\approx_l$	$\Leftarrow$	$\stackrel{?}{=}$
Vote	B	A	A	50% A, 50% B

The Applied Pi Calculus [?]

Syntax

$P, Q, R :=$	processes
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction ("new")
$\texttt{if } M = N \texttt{ then } P \texttt{ else } Q$	conditional
$\texttt{in}(u, x).P$	message input
$\texttt{out}(u, x).P$	message output
$\{^M/_x\}$	substitution

Modeling Voting Protocols

Definition (Voting Process)

A voting process is a closed process

$$\nu\tilde{n}.(V\sigma_{id_1}\sigma_{v_1}|\dots|V\sigma_{id_n}\sigma_{v_n}|A_1|\dots|A_l)$$

where

- $\tilde{n}$ is a set of restricted names,
- σ_{id_i} is a substitution assigning the identity to a voter process,
- σ_{v_i} specifies the vote and
- A_j are the election authorities which are required to be honest.

Vote-Privacy (VP) in the Applied Pi Calculus

Definition (Vote-Privacy (VP))

A voting protocol ensures *Vote-Privacy (VP)* if for any two instances $VP_A = \nu \tilde{n}.(V\sigma_{id_1}\sigma_{v_1^A} \mid \ldots \mid V\sigma_{id_n}\sigma_{v_n^A} \mid A_1 \mid \ldots \mid A_l)$ and $VP_B = \nu \tilde{n}.(V\sigma_{id_1}\sigma_{v_1^B} \mid \ldots \mid V\sigma_{id_n}\sigma_{v_n^B} \mid A_1 \mid \ldots \mid A_l)$ we have

$$VP_A|_{res} \approx_l VP_B|_{res} \Rightarrow VP_A \approx_l VP_B.$$

Link to existing definitions: Equality of Votes (EQ)

	Alice	Bob	$\cdots$		Result
Vote	V_1^A	V_2^A	$\cdots$		Result 1
		$\exists\ \pi$		$\Leftrightarrow$	$=$
Vote	$V^B_{\pi(1)}$	$V^B_{\pi(2)}$	$\cdots$		Result 2

Link to existing definitions, cont'd

Theorem (Equivalence of Privacy Definitions)

If a protocol respects Equality of Votes (EQ), then Vote-Privacy (VP) and Swap-Privacy (SwP) are equivalent:

$$SwP \xleftrightarrow{EQ} VP$$

Case Study

Eliasson and Zúquete [?]: different versions of Fujioka et al. [?] implementing weighted votes, for example using multiple ballots per voter. Manual proof to show that

$$VP_A|_{res} \approx_l VP_B|_{res} \Rightarrow \sum_{i=1}^{n} V_i^A * w_i = \sum_{i=1}^{n} V_i^B * w_i.$$

ProVerif [?] to establish the following, which gives (VP).

$$\sum_{i=1}^{n} V_i^A * w_i = \sum_{i=1}^{n} V_i^B * w_i \Rightarrow VP_A \approx_l VP_B$$

Plan

Existing Definition: Swap-Receipt-Freeness (SwRF) [?]

Again: Observational equivalence between two situations, but Alice tries to create a receipt or a fake.

Mallory

Alice Bob

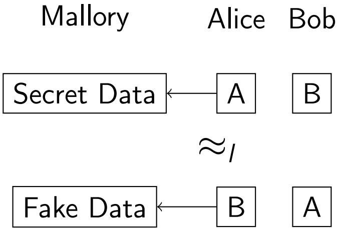
A B

$\approx_l$

B A

Existing Definition: Swap-Receipt-Freeness (SwRF) [?]

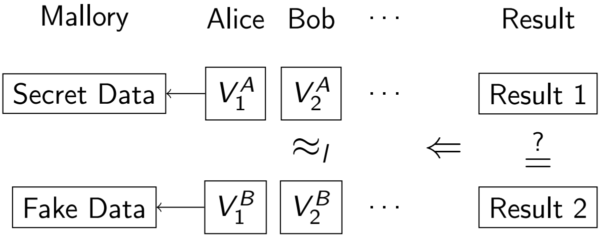
Again: Observational equivalence between two situations, but Alice tries to create a receipt or a fake.



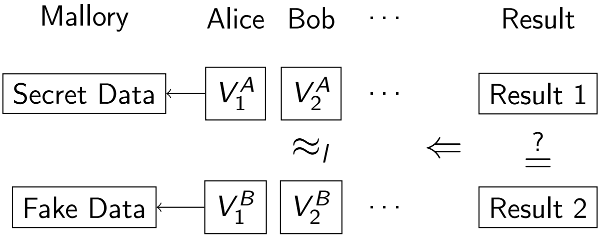
Single-Voter Receipt Freeness (SRF)

Mallory	Alice	Bob	$\cdots$		Result
	V_1^A	V_2^A	$\cdots$		Result 1
		$\approx_l$		$\Leftarrow$	$\stackrel{?}{=}$
	V_1^B	V_2^B	$\cdots$		Result 2

Single-Voter Receipt Freeness (SRF)

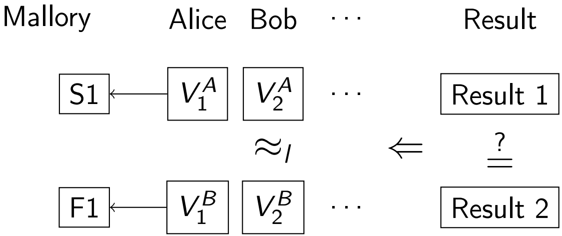


Single-Voter Receipt Freeness (SRF)

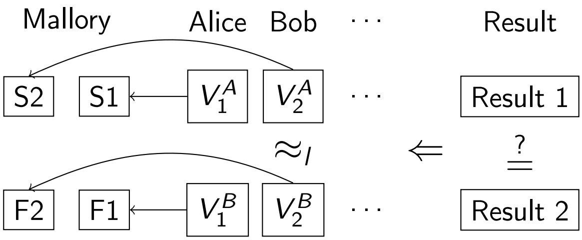


If a protocol respects (EQ), then (SRF) and (SwRF) are equivalent.

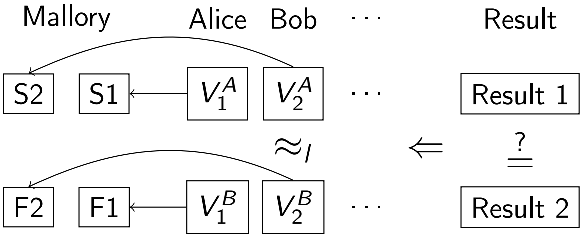
Multi-Voter Receipt Freeness (MRF)



Multi-Voter Receipt Freeness (MRF)

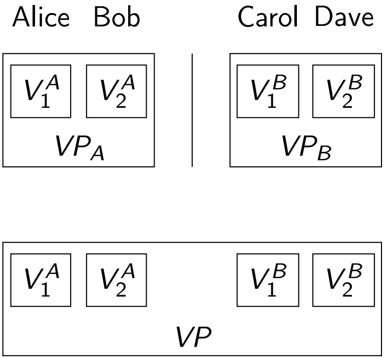


Multi-Voter Receipt Freeness (MRF)

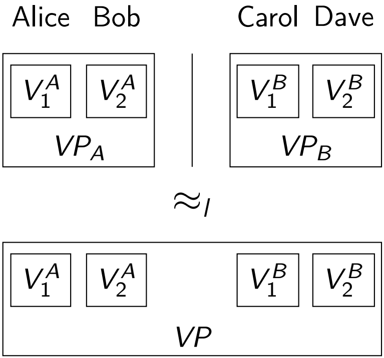


Multi-Voter Receipt Freeness (MRF) implies Single-Voter Receipt Freeness (SRF).

Link between (SRF) and (MRF): Modularity (Mod)



Link between (SRF) and (MRF): Modularity (Mod)



Link between (SRF) and (MRF) cont'd: Correctness (Cor)

	Alice	Bob	⋯	Result
Vote	V_1^A	V_2^A	⋯	Result 1
Vote	V_1^B	V_2^B	⋯	Result 2

Link between (SRF) and (MRF) cont'd: Correctness (Cor)

	Alice	Bob	$\cdots$	Result
Vote	V_1^A	V_2^A	$\cdots$	Result 1
	$\forall i\ V_i^A = V_i^B$			
Vote	V_1^B	V_2^B	$\cdots$	Result 2

Link between (SRF) and (MRF) cont'd: Correctness (Cor)

	Alice	Bob	$\cdots$		Result
Vote	V_1^A	V_2^A	$\cdots$		Result 1
	$\forall i \; V_i^A = V_i^B$			$\Rightarrow$	
Vote	V_1^B	V_2^B	$\cdots$		Result 2

Link between (SRF) and (MRF) cont'd: Correctness (Cor)

	Alice	Bob	$\cdots$		Result
Vote	V_1^A	V_2^A	$\cdots$		Result 1
	$\forall i\ V_i^A = V_i^B$			$\Rightarrow$	$=$
Vote	V_1^B	V_2^B	$\cdots$		Result 2

Link between (SRF) and (MRF) cont'd: Correctness (Cor)

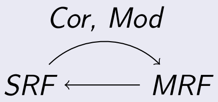
	Alice	Bob	$\cdots$		Result
Vote	V_1^A	V_2^A	$\cdots$		Result 1
	$\forall i\ V_i^A = V_i^B$			$\Rightarrow$	$=$
Vote	V_1^B	V_2^B	$\cdots$		Result 2

Equality of Votes (EQ) implies Correctness (Cor).

Link between (SRF) and (MRF) cont'd

Theorem (Equivalence of Single- and Multi-Voter Coercion)

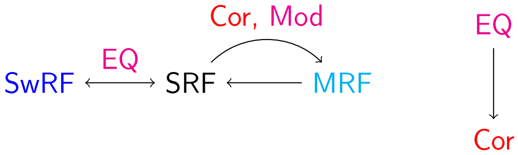
If a protocol is modular and correct, Single-Voter Receipt Freeness and Multi-Voter Receipt Freeness are equivalent.



Case Study

Protocol by Okamoto [?]:

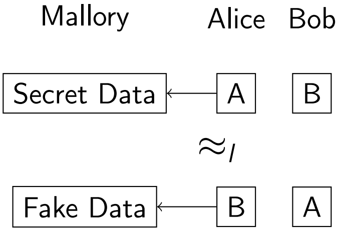
- (SwRF) shown before [?].
- We prove (EQ) and (Mod)
- and obtain Multi-Voter Receipt Freeness (MRF):



Plan

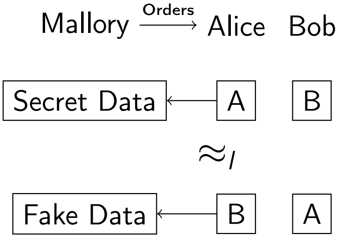
Existing Definition: Swap-Coercion-Resistance (SwCR) [?]

Observational equivalence between two situations, but Alice is under control by Mallory or only pretends to be so.

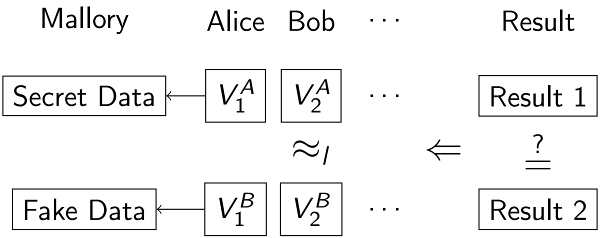


Existing Definition: Swap-Coercion-Resistance (SwCR) [?]

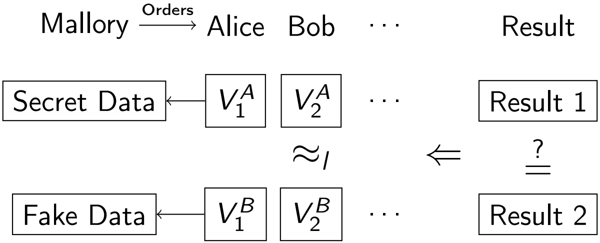
Observational equivalence between two situations, but Alice is under control by Mallory or only pretends to be so.



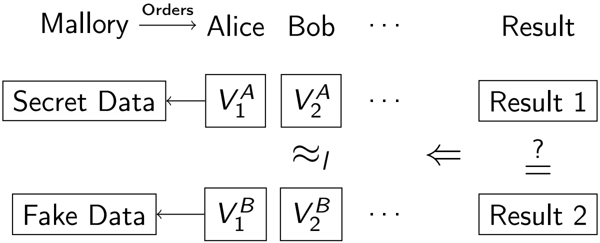
Single-Voter Coercion-Resistance (SCR)



Single-Voter Coercion-Resistance (SCR)

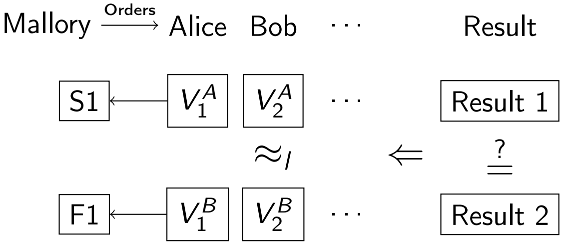


Single-Voter Coercion-Resistance (SCR)

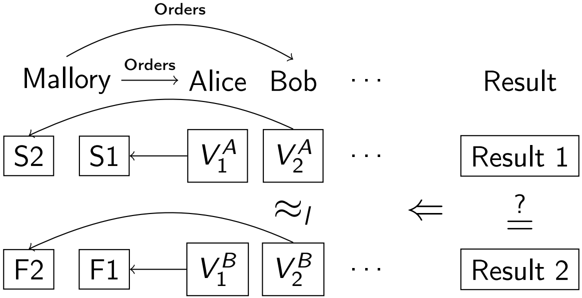


If a protocol respects (EQ), then (SCR) and (SwCR) are equivalent.

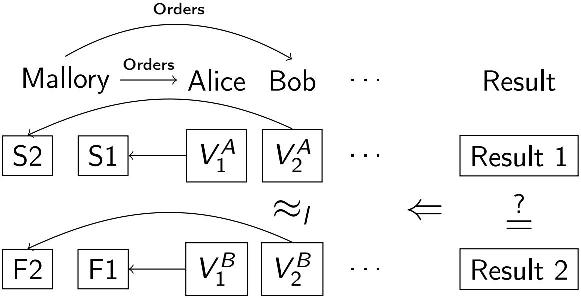
Multi-Voter Coercion-Resistance (MCR)



Multi-Voter Coercion-Resistance (MCR)



Multi-Voter Coercion-Resistance (MCR)

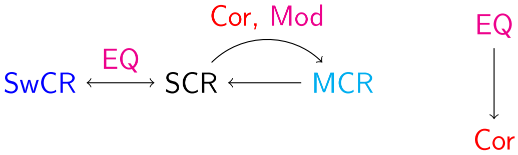


If a protocol is modular and correct, Single-Voter Coercion-Resistance and Multi-Voter Coercion-Resistance are equivalent.

Case Study

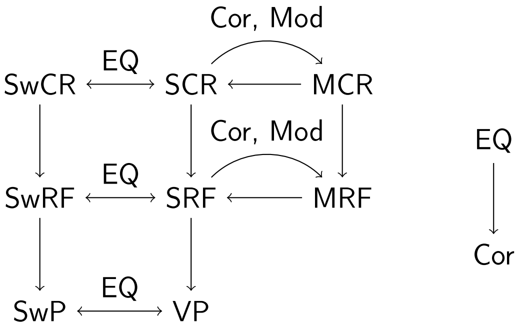
Bingo Voting [?]:

- (SwCR) shown before [?].
- We prove (EQ) and (Mod)
- and obtain Multi-Voter Coercion-Resistance (MCR):



Plan

Relations among the notions



Conclusion

- Generalized definition for weighted votes
- Definition of Single- and Multi-Voter Receipt-Freeness and Coercion
- Proofs of Equivalence
- Case studies:
  - Variant of Fujioka et al. [?]: Vote-Privacy (VP)
  - Okamoto [?]: Multi-Voter Receipt Freeness (MRF)
  - Bingo Voting [?]: Multi-Voter Coercion-Resistance (MCR)

Thank you for your attention!

Questions?

Cryptographic Primitives

- *Commitments:* open(commit(v, r), r) = v
- *Signatures:* checksign(sign(x, sk(Y)), pk(Y)) = ok
- *Blind signatures:* unblind(sign(blind(x, r), key), r) = sign(x, r)

Protocol Description [?]

The protocol is split into three phases:

- Eligibility Check
- Voting
- Counting

Authorities:

- Administrator
- Collector

Assumptions:

- Anonymous channel to the collector

Eligibility Check

Bob

Administrator

Eligibility Check

Bob Administrator

sign(blind(commit(B, r_1^B), r_2^B), sk(B)), Identity(B)

$\longrightarrow$

Eligibility Check

Bob Administrator

$\text{sign}(\text{blind}(\text{commit}(B, r_1^B), r_2^B), \text{sk}(B)), \text{Identity}(B)$

$\longrightarrow$

$\text{sign}(\text{blind}(\text{commit}(B, r_1^B), r_2^B), \text{sk}(Ad))$

$\longleftarrow$

Eligibility Check

Bob — Administrator

Bob → Administrator: sign(blind(commit(B, r_1^B), r_2^B), sk(B)), Identity(B)

Administrator → Bob: sign(blind(commit(B, r_1^B), r_2^B), sk(Ad))

sign(commit(V, r_1^B), sk(Ad))

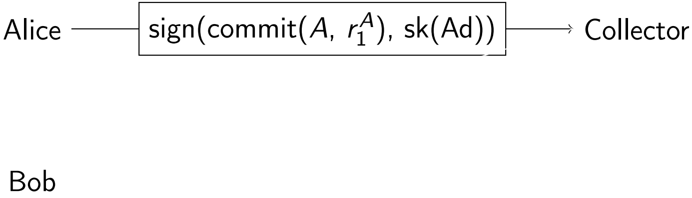
Voting Phase

Alice

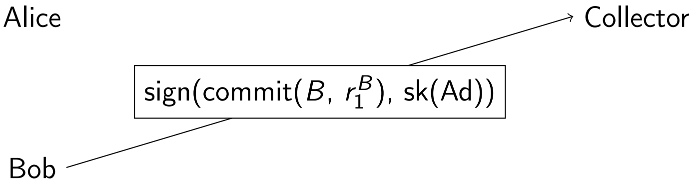
Collector

Bob

Voting Phase



Voting Phase



Couting Phase

Alice

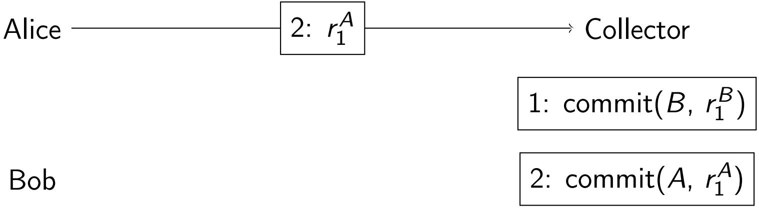
Bob

Collector

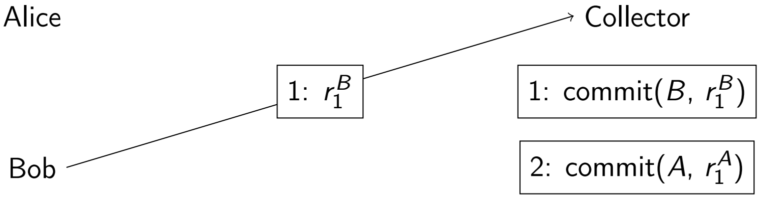
1: $\text{commit}(B,\ r_1^B)$

2: $\text{commit}(A,\ r_1^A)$

Couting Phase



Couting Phase



Couting Phase

Alice

Bob