CDS Composition of Multi-Round Protocols

Masayuki Abe (NTT Social Informatics Laboratories)
Andrej Bogdanov (University of Ottawa)
Miyako Ohkubo (NICT)
Alon Rosen (Bocconi University and Reichman University)
Zehua Shang (Kyoto University)
Mehdi Tibouchi (NTT Social Informatics Laboratories)

Sigma protocol [Cramer'96]

P		V
$(x, w) \in R$		x
$a \leftarrow \mathsf{A}(x; r)$	$\xrightarrow{\quad a \quad}$	
	$\xleftarrow{\quad e \quad}$	$e \leftarrow \$$
$z \leftarrow \mathsf{Z}(x, r, e, w)$	$\xrightarrow{\quad z \quad}$	$1/0 \leftarrow \mathsf{Verif}(x, a, e, z)$

Sigma protocol [Cramer'96]

- Completeness:
  - $R(x, w) = 1 \rightarrow$ Verifier accepts
- 2-Special Soundness:
  - $\mathrm{Ext}(a, e, z, e', z') \rightarrow w$
- (Special) Honest Verifier Zero Knowledge:
  - $\mathrm{Sim}(x, e) \rightarrow (a, z)$
- Generalization:
  - Multi-round, $(k_1, \dots, k_\mu)$-special sound PCIP

The CDS OR-composition [CDS94]

Relation: $(x_1 \vee x_2; w_1)$
Ingredients: Σ-protocols + secret sharing

$x_1; w_1$	x_2	
$a_1 \leftarrow A(x_1; r_1)$	$e_2 \leftarrow \$$ $(a_2, z_2) \leftarrow \mathrm{Sim}(x_2, e_2)$	$\{a_1, a_2\}$ →

$e_1 = e - e_2$ ← $e \leftarrow \$$

$z_1 \leftarrow Z(x_1, r_1, e_1, w_1)$ → $\{e_1, e_2, z_1, z_2\}$

The CDS OR-composition [CDS94]

Relation: $(x_1 \vee x_2; w_1)$

Ingredients: Σ-protocols + secret sharing

Linear proof size

$x_1; w_1$	x_2	
$a_1 \leftarrow A(x_1; r_1)$	$e_2 \leftarrow \$$ $(a_2, z_2) \leftarrow \mathrm{Sim}(x_2, e_2)$	$\{a_1, a_2\}$ →

$e_1 = e - e_2$ ← $e \leftarrow \$$

$z_1 \leftarrow Z(x_1, r_1, e_1, w_1)$ → $\{e_1, e_2, z_1, z_2\}$

The CDS OR-composition [CDS94]

Relation: $(x_1 \vee x_2; w_1)$

Ingredients: Σ-protocols + secret sharing

Linear proof size

Security preserving

$x_1; w_1$	x_2
$a_1 \leftarrow A(x_1; r_1)$	$e_2 \leftarrow \$$ $(a_2, z_2) \leftarrow \mathrm{Sim}(x_2, e_2)$

$\{a_1, a_2\}$ →

$e \leftarrow \$$ ←

$$e_1 = e - e_2$$

$$z_1 \leftarrow Z(x_1, r_1, e_1, w_1)$$

$\{e_1, e_2, z_1, z_2\}$ →

The CDS OR-composition [CDS94]

Relation: $(x_1 \vee x_2; w_1)$

Ingredients: Σ-protocols + secret sharing

Linear proof size

Security preserving

Precomputable (if x_2 known)

$x_1; w_1$	x_2	
$a_1 \leftarrow A(x_1; r_1)$	$e_2 \leftarrow \$$ $(a_2, z_2) \leftarrow \mathrm{Sim}(x_2, e_2)$	$\{a_1, a_2\}$ →
$e_1 = e - e_2$		← $e \leftarrow \$$
$z_1 \leftarrow Z(x_1, r_1, e_1, w_1)$		$\{e_1, e_2, z_1, z_2\}$ →

The CDS OR-composition [CDS94]

Relation: $\{x_{i\in[n]}; w_{j\in A\in\Gamma}\}$, $\Gamma \in$ MSP (Monotone Span Program)

Ingredients: n Σ-protocol Π + SS

$i \in \mathrm{A}$	$j \notin \mathrm{A}$	
$a_i \leftarrow A(x_i; r_i)$	$e_j \leftarrow \$$ $(a_j, z_j) \leftarrow \mathrm{Sim}(x_j, e_j)$	$\{a_{i\in[n]}\}$ →
$\{e_{i\in[n]}\} \leftarrow \mathrm{SS.Complete}_{\Gamma^*}(e, \{e_j\})$		← $e \leftarrow \$$
$z_i \leftarrow Z(x_i, r_i, e_i, w_i)$		$\{e_{i\in[n]}, z_{i\in[n]}\}$ →

Generalizations of Sigma-protocols

- Generalizations of Sigma-protocols:
  - 2-special sound $\Longrightarrow$ k-special sound
  - 3-round $\Longrightarrow$ $2\mu + 1$-round

- Why generalizations?
  - Better efficiency
  - SNARKs
  - Compressed Sigma protocol [AC20, ACK21]
  - …

Generalization of CDS composition

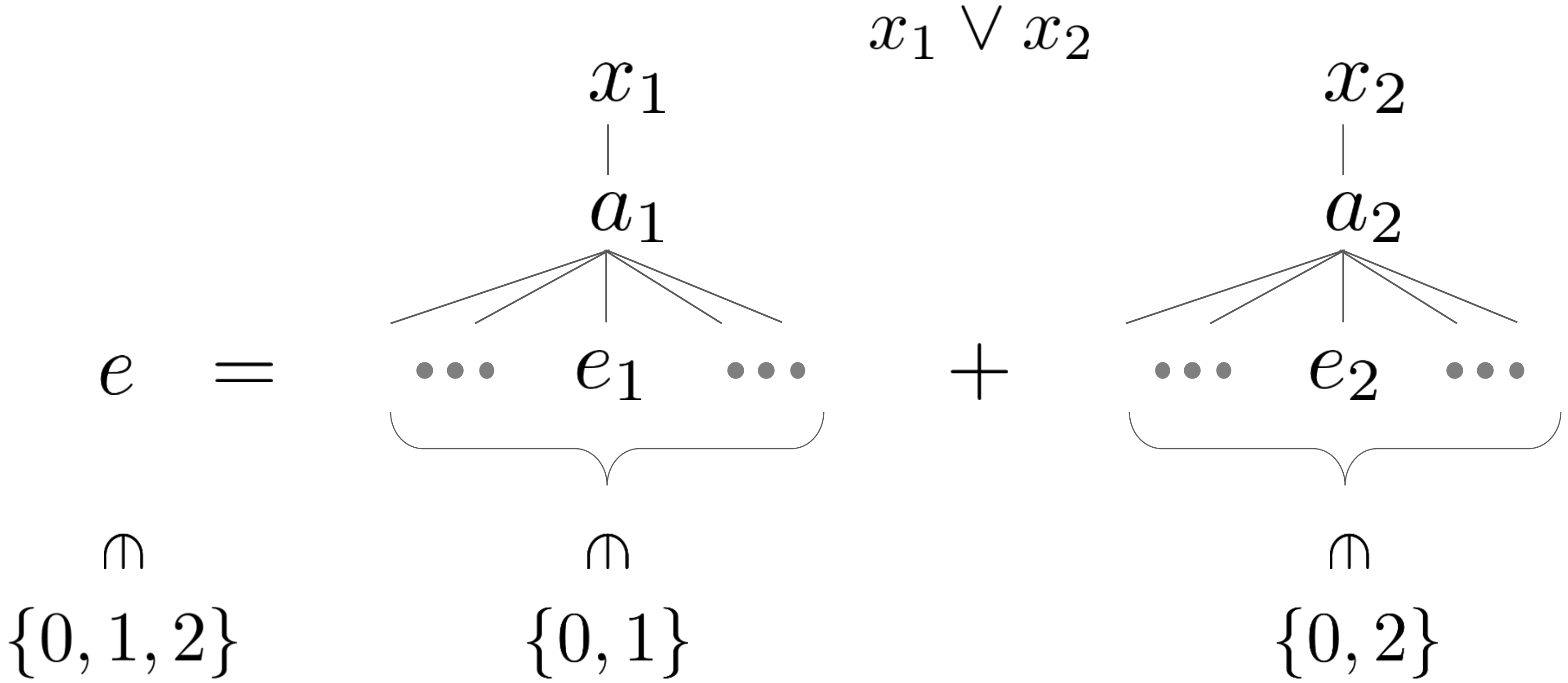
- Does CDS apply to $2\mu + 1$-round $(k_1, \ldots, k_\mu)$-special sound protocols?

Special Soundness	Number of Rounds	Expressibility	CDS works?
2-special sound	3	MSP	✓
$\boldsymbol{k}$-special sound	3	OR	×
2-special sound	$\boldsymbol{2\mu + 1}$	OR	×

- Neither of generalizations work below:
  - 2-special sound $\Longrightarrow$ k-special sound
  - 3-round $\Longrightarrow$ $2\mu + 1$-round

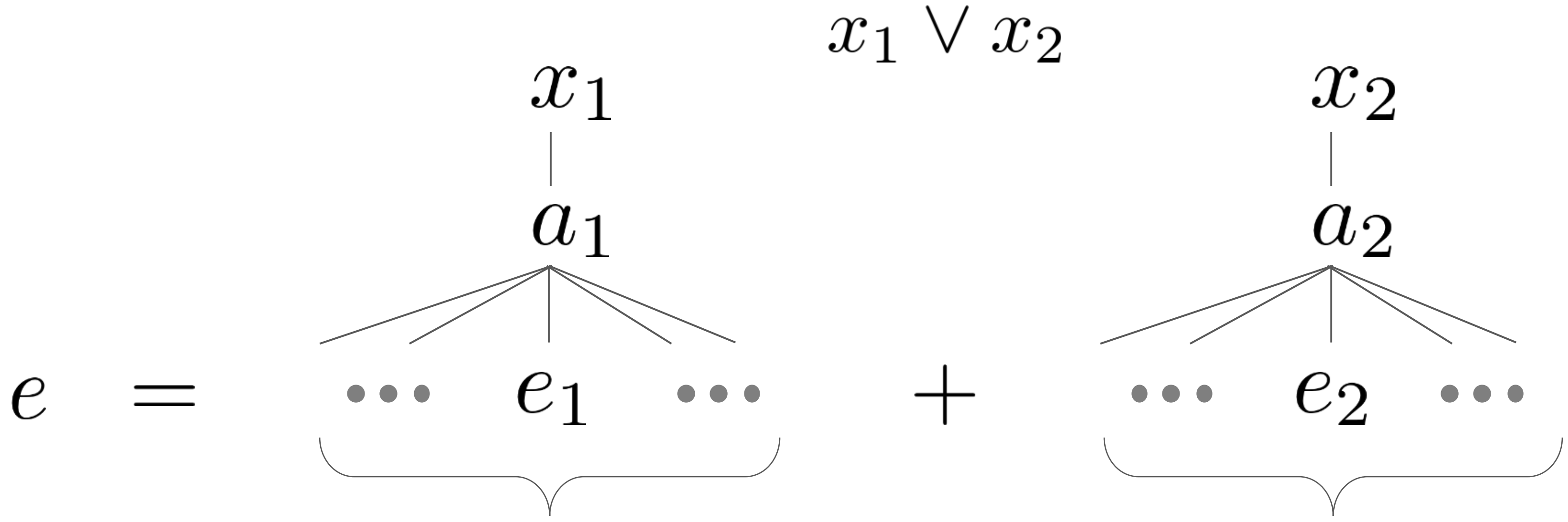
CDS fails- Case 1 (k-special soundness)

- e.g. 3-special soundness (Stern's Protocol)



CDS fails- Case 1 (k-special soundness)

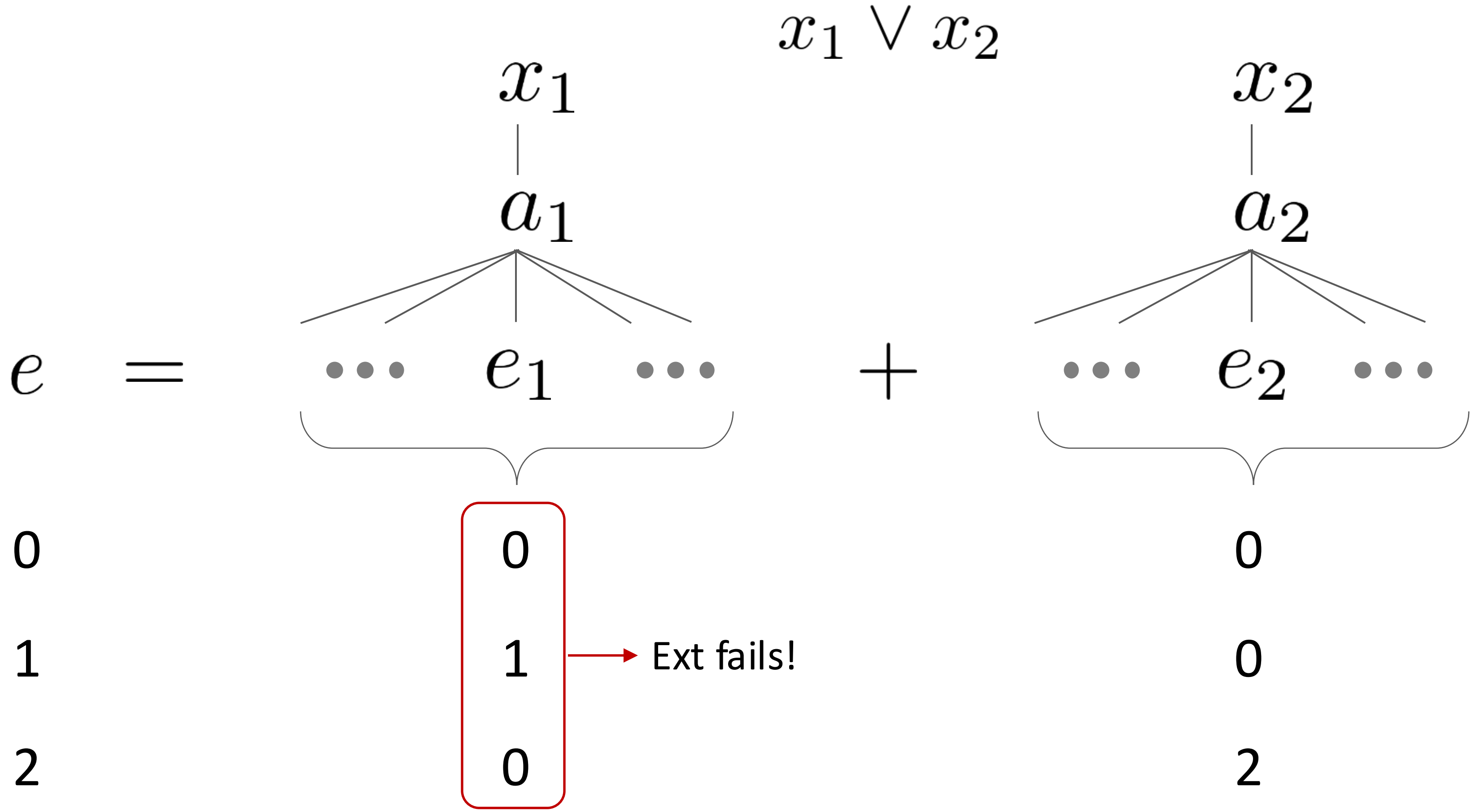
- e.g. 3-special soundness (Stern's Protocol)



e	e_1	e_2
0	0	0
1	1	0
2	0	2

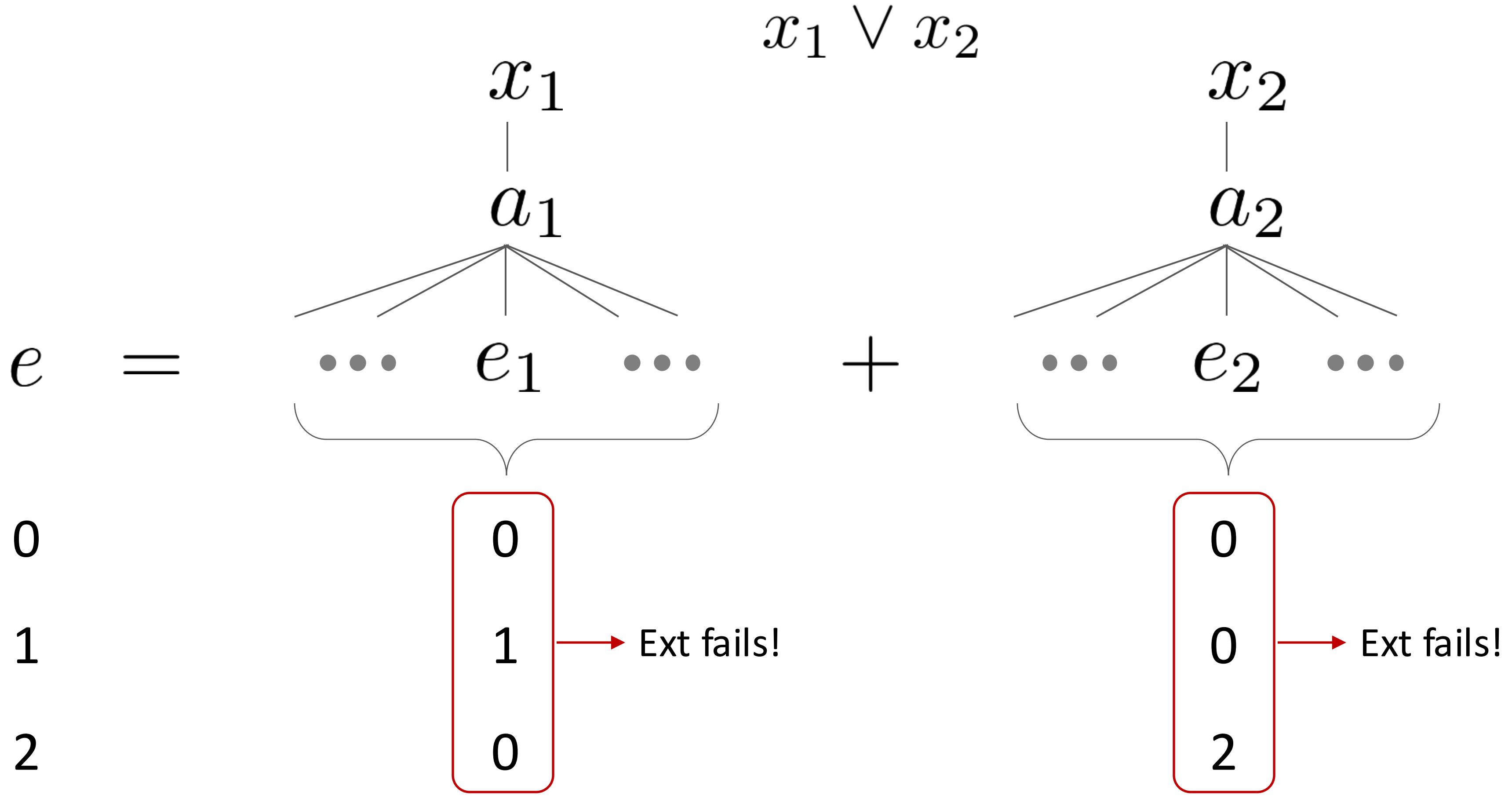
CDS fails- Case 1 (k-special soundness)

- e.g. 3-special soundness (Stern's Protocol)



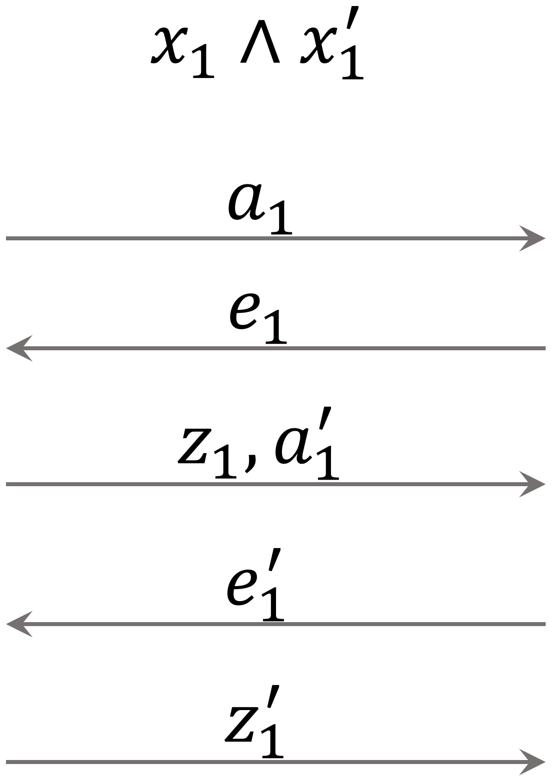
CDS fails- Case 1 (k-special soundness)

- e.g. 3-special soundness (Stern's Protocol)



CDS fails- Case 2 ($2\mu + 1$-round)

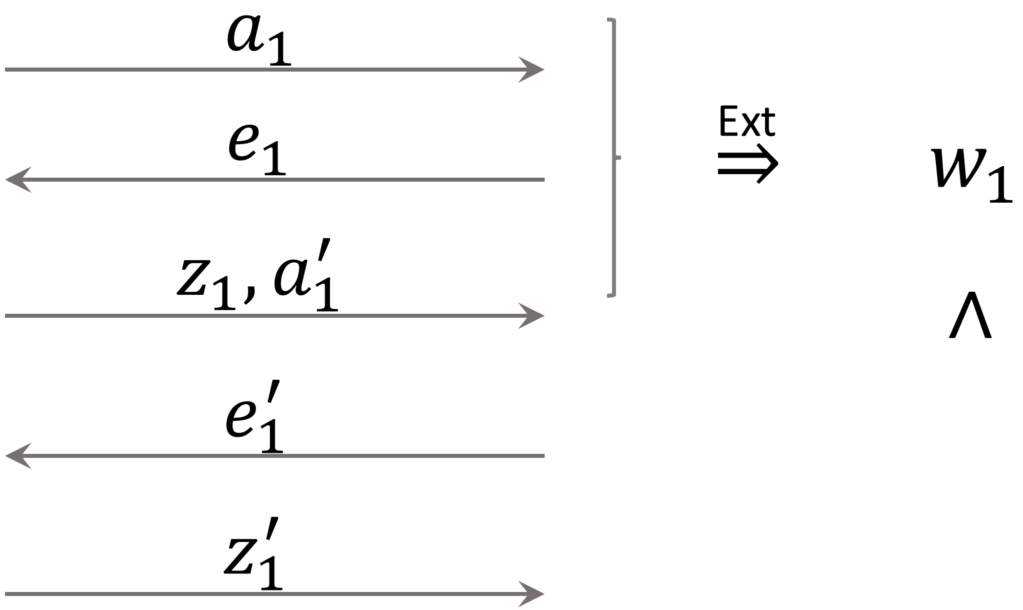
- A 5-round protocol for relation $x_1 \wedge x_1'$:



CDS fails- Case 2 ($2\mu + 1$-round)

- A 5-round protocol for relation $x_1 \wedge x_1'$:

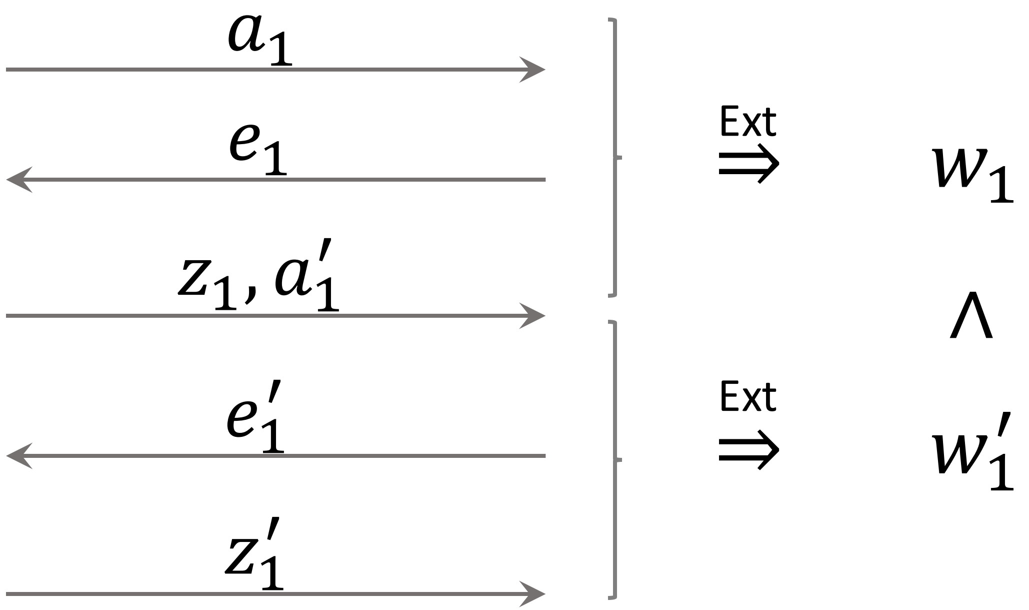
$x_1 \wedge x_1'$



CDS fails- Case 2 ($2\mu + 1$-round)

- A 5-round protocol for relation $x_1 \wedge x_1'$:

$$x_1 \wedge x_1'$$



CDS fails- Case 2 ($2\mu + 1$-round)

- An OR-proof for $(x_1 \wedge x_1') \vee (x_2 \wedge x_2')$:

$x_1 \wedge x_1'$		$x_2 \wedge x_2'$		
a_1		a_2		
e_{1a}	$+$	e_2	$=$	e_a
z_1, a_1'		z_2, a_2'		
e_{1a}'	$+$	e_2'	$=$	e_a'
z_1' …		z_2'		

CDS fails- Case 2 ($2\mu + 1$-round)

- An OR-proof for $(x_1 \wedge x_1') \vee (x_2 \wedge x_2')$:

$x_1 \wedge x_1'$		$x_2 \wedge x_2'$		
a_1		a_2		
e_{1a} e_{1b}	$+$	e_2	$=$	e_a e_b
z_1, a_1'		z_2, a_2'		
e_{1a}'	$+$	e_2'	$=$	e_a'
z_1' …		z_2'		

CDS fails- Case 2 ($2\mu + 1$-round)

- An OR-proof for $(x_1 \wedge x_1') \vee (x_2 \wedge x_2')$:

$x_1 \wedge x_1'$ $\qquad\qquad$ $x_2 \wedge x_2'$

a_1 $\qquad\qquad$ a_2

$e_{1a} \quad e_{1b} \quad + \quad e_2 \quad = \quad e_a \quad e_b$

z_1, a_1' $\qquad\qquad$ z_2, a_2'

$e_{1a}' \quad e_{1b}' \quad + \quad e_2' \quad = \quad e_a' \quad e_b'$

z_1' $\quad \ldots \quad$ z_2'

CDS fails- Case 2 ($2\mu + 1$-round)

- An OR-proof for $(x_1 \wedge x_1') \vee (x_2 \wedge x_2')$:

$x_1 \wedge x_1'$ | $x_2 \wedge x_2'$

a_1 | a_2

w_1 ← Ext ← $e_{1a}\ \ e_{1b}$ $+$ e_2 $=$ $e_a\ \ e_b$

$\wedge$ | z_1, a_1' | z_2, a_2'

w_1' ← Ext ← $e_{1a}'\ \ e_{1b}'$ $+$ e_2' $=$ $e_a'\ \ e_b'$

z_1' … | z_2'

Extraction succeeds

CDS fails- Case 2 ($2\mu + 1$-round)

- Suppose prover has w_1, w_1', w_2, w_2':

$x_1 \wedge x_1'$ $\quad\quad$ $x_2 \wedge x_2'$

a_1 $\quad\quad$ a_2

w_1 ← Ext $\quad$ $e_{1a} \quad e_{1b}$ $\quad + \quad$ e_2 $\quad = \quad$ $e_a \quad e_b$

$\wedge$ $\quad$ z_1, a_1' $\quad\quad$ z_2, a_2'

e_1' $\quad + \quad$ e_{2a}' $\quad = \quad$ e_a'

z_1' $\quad$ … $\quad$ z_2'

CDS fails- Case 2 ($2\mu + 1$-round)

- Suppose prover has w_1, w_1', w_2, w_2':

$x_1 \wedge x_1'$ $\qquad$ $x_2 \wedge x_2'$

a_1 $\qquad$ a_2

w_1 ← Ext $\boxed{e_{1a} \quad e_{1b}}$ $+$ e_2 $=$ $e_a \quad e_b$

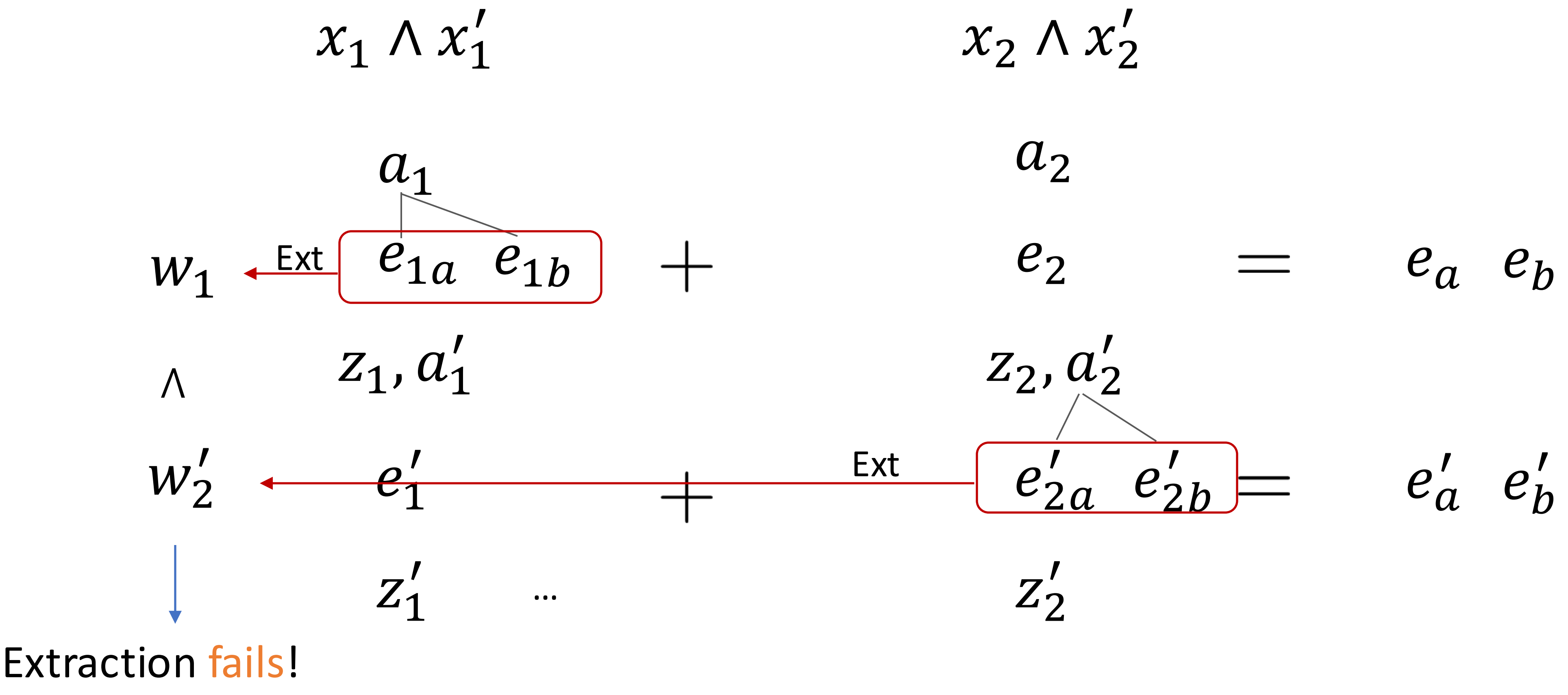
$\wedge$ $\qquad$ z_1, a_1' $\qquad$ z_2, a_2'

e_1' $+$ $e_{2a}' \quad e_{2b}'$ $=$ $e_a' \quad e_b'$

z_1' $\quad \dots \quad$ z_2'

CDS fails- Case 2 ($2\mu + 1$-round)

- Suppose prover has w_1, w_1', w_2, w_2':



Our Result

- Our result:

Composition method	Special Soundness	Number of Rounds	Expressibility
CDS	2-special sound	3	MSP
Ours	**$(k_1, \dots, k_\mu)$-special sound**	$2\mu + 1$	**mNC[1]**

- Observation:
  - CDS fails because the prover is given too much freedom on choosing challenges
- Our approach:
  - Let the prover commit to simulated challenges

Use of dual-mode commitments

- We use dual-mode commitments.
  - Plain model
  - Binding mode: perfect binding, comp. hiding
  - Hiding mode: perfect hiding, comp. binding, equivocable
  - Mode indistinguishable

- Prove: If simulated, Com works in binding mode
- And Coms are indistinguishable among all positions

Our Composition

Relation: $(x_1 \vee x_2; w_1)$

Ingredients: PCIPs + SS + dual-mode Com. (e.g. 5-round OR-proof)

$x_1; w_1$	x_2	
$a_1 \leftarrow A(x_1; r_1)$	$e_2, e_2' \leftarrow \$$	
$(c_1, d_1) \leftarrow \mathrm{Com}(0\|\|0)$	$(a_2, z_2, z_2') \leftarrow \mathrm{Sim}(x_2, e_2, e_2')$	$\{a_1, a_2, c_1, c_2\}$ →
	$(c_2, d_2) \leftarrow \mathrm{Com}(e_2\|\|e_2')$	

$e \leftarrow \$$ ←

$e_1 = e - e_2$

$z_1 \leftarrow Z(x_1, r_1, e_1, w_1)$

$\{e_1, e_2, z_1, z_2\}$ →

$e' \leftarrow \$$ ←

$e_1' = e' - e_2'$

$d_1' \leftarrow \mathrm{Equiv}(c_1, e_1\|\|e_1', 0\|\|0)$

$z_1' \leftarrow Z(x_1, r_1, e_1', e_1, w_1)$

$\{e_1', e_2', z_1', z_2', d_1', d_2\}$ →

Our Composition

Relation: $(x_1 \vee x_2; w_1)$

Ingredients: PCIPs + SS + dual-mode Com. (e.g. 5-round OR-proof)

$x_1; w_1$	x_2
	$e_2, e_2' \leftarrow \$$
$a_1 \leftarrow A(x_1; r_1)$	$(a_2, z_2, z_2') \leftarrow \mathrm{Sim}(x_2, e_2, e_2')$
$(c_1, d_1) \leftarrow \mathrm{Com}(0\|\|0)$	$(c_2, d_2) \leftarrow \mathrm{Com}(e_2\|\|e_2')$

Prove: at least one of them are **Binding**

$z_1 \leftarrow Z(x_1, r_1, e$

$e_1' = e' - e_2'$

$d_1' \leftarrow \mathrm{Equiv}(c_1, e_1\|\|e_1', 0\|\|0)$

$z_1' \leftarrow Z(x_1, r_1, e_1', e_1, w_1)$

$\{a_1, a_2, c_1, c_2\}$ →

← $e \leftarrow \$$

$\{e_1, e_2, z_1, z_2\}$ →

← $e' \leftarrow \$$

$\{e_1', e_2', z_1', z_2', d_1', d_2\}$ →

Complexity of adversarial structure

- Subproof gets more complicated beyond simple OR
- For simple OR:
  - Prove: "at least one of the Coms are binding"
- For general access structure Γ:
  - Prove: "Binding Coms are in a structure Γ'"
  - What is Γ'? Complexity of Γ'?

Complexity of adversarial structure

- We call Γ' the adversarial access structure.
- Negative:
  - Assuming NP $\subsetneq$ P/poly, $\exists\Gamma \in$ MSP s.t. Γ' blowup in circuit size.
- Positive:
  - If Γ is computed by a **read-once** formula (e.g. mNC^1), then Γ' can be computed in polynomial time.
  - Examples in mNC^1 :
    - t-out-of-n Threshold
    - Thresholds of thresholds
    - Ranked Choice Voting

Challenge Space vs Share Size

- Issue: Share size often exceeds max length of challenge space

- Solution [CDS94]: Parallel Repetition
  - Challenge space $C \Rightarrow C^t$
  - Works for 2-special sound sigma-protocols
  - 2-special soundness preserves in parallel repetition

- Fact: k-special soundness does not preserve in parallel repetition
  - k-special soundness $\xRightarrow{\text{t fold}} (k-1)^t + 1$-special soundness

Challenge Space vs Share Size

- Our relaxation: **statistical** k-special soundness
  - Observation: Number of bad transcripts are negligible

- Definition: $\mathrm{Ext}(\mathrm{transcript}) \to w$ fails only for negl. probability κ
  - κ depends on the choices of challenges
  - $(k_1, \ldots, k_\mu)$-special soundness $\overset{\mathrm{t\ fold}}{\Longrightarrow}$ **statistical** $(k_1, \ldots, k_\mu)$-special soundness.

Remark: essentially the same notion is introduced in [AAB+24] (ePrint:2024/311) in this conference

Conclusion

- Generalize CDS composition for multi-round PCIP
  - Plain model
  - Simulation precomputable
  - Soundness & round preserving
- Complexity of adversarial structure
  - mNC^1
- Challenge Space vs Share Size
  - statistical $(k_1, \ldots, k_\mu)$-special soundness

Thanks!