

Critical Rounds in Multi-Round Proofs: Proof of Partial Knowledge and Trapdoor Commitments

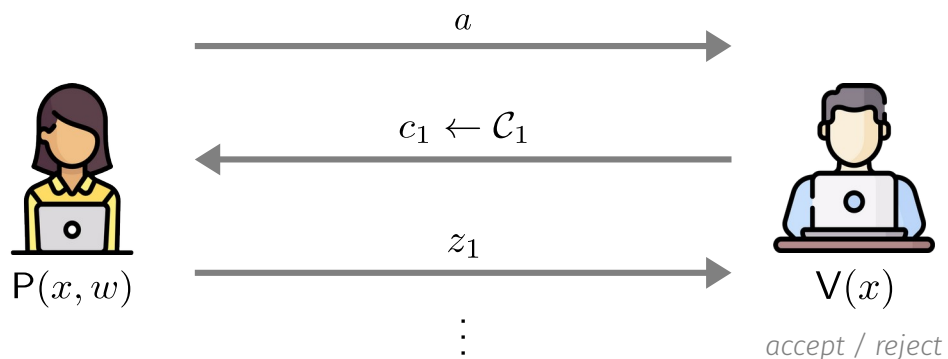
Masayuki Abe, David Balbás, Dung Bui, Miyako Ohkubo,
Zehua Shang, Akira Takahashi, Mehdi Tibouchi

NY Crypto Day @ J.P.Morgan

From Eurocrypt 2026

ePrint 2024/1766

Public-Coin Proof Systems



Statement x , **witness** w with $R(x, w) = 1$. **Public coin:** the verifier doesn't maintain any secret state

Soundness: a prover that makes V accept must know a witness w

Zero-knowledge: real vs. ideal

Real world



$\approx$

Ideal world



a simulator, without the witness

V learns nothing beyond the validity of x

Constructive Use of the ZK Simulator

The usual view: a proof tool

The simulator lives in the **ideal world** of the security proof. Is it just a hypothetical entity?

The constructive view: a building block

No. The simulator can be run as part of a construction in the **real world**!

Well-known uses of ZK simulator of 3-round proofs:

Proof of Partial Knowledge
[Cramer-Damgård-Schoenmaker 94]

Trapdoor Commitments
[Damgård90, Fischlin01]

Zero-knowledge: real vs. ideal

Real world



the prover uses the witness

$\approx$

Ideal world

$\text{Sim}(x) \longrightarrow (a, c_1, z_1, \dots)$

a simulator, without the witness

$\mathcal{V}$ learns nothing beyond the validity of x

Can we generalize the constructive uses of the ZK simulator to the multi-round setting?

Our Contributions

Yes, for protocols with a **critical round**: the simulator needs only one challenge in advance.

1. Critical-Round ZK

- The simulator needs only **one** challenge in advance, the critical one c_{i^*}
- Satisfied by several practical proofs:
 - MPC-in-the-Head (KKW18)
 - Plonk
 - Bulletproofs
 - compressed Σ -protocols

2. Proof of Partial Knowledge

- Can prove knowledge of witness for a subset of many public statements
- **Multi-Round CDS (MR-CDS)**:
 - no extra assumptions,
 - constant number of statements
- **Multi-Round Share-then-Hash (MR-StH)**: polynomially many statements, from a collision-resistant hash

3. Trapdoor Commitments

- Equivocation without programming the random oracle
- Computationally binding assuming the hardness of relation R supported by the proof system.

Roadmap

1

Recap: constructive use of the ZK simulator

for Σ -protocols, and why the naive multi-round extension fails

2

Critical-round SHVZK

one challenge in advance

3

Multi-round proof of partial knowledge

MR-CDS and MR-StH

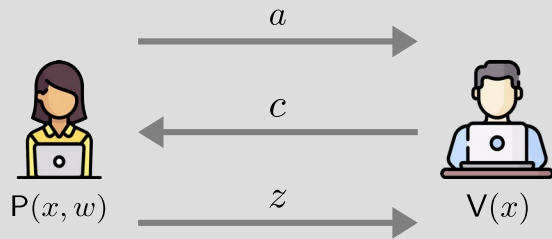
4

Trapdoor commitments

from multi-round proofs

Recap: Σ -Protocols

Syntax: three moves



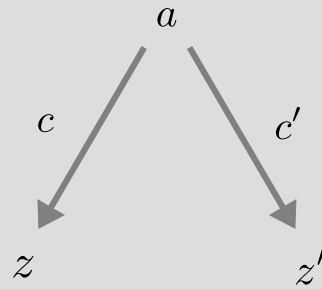
Prover algorithms

$(st, a) \leftarrow A(x, w)$
 $z \leftarrow Z(st, c)$

Verifier accepts iff

$V(x, a, c, z) = 1$

2-special soundness

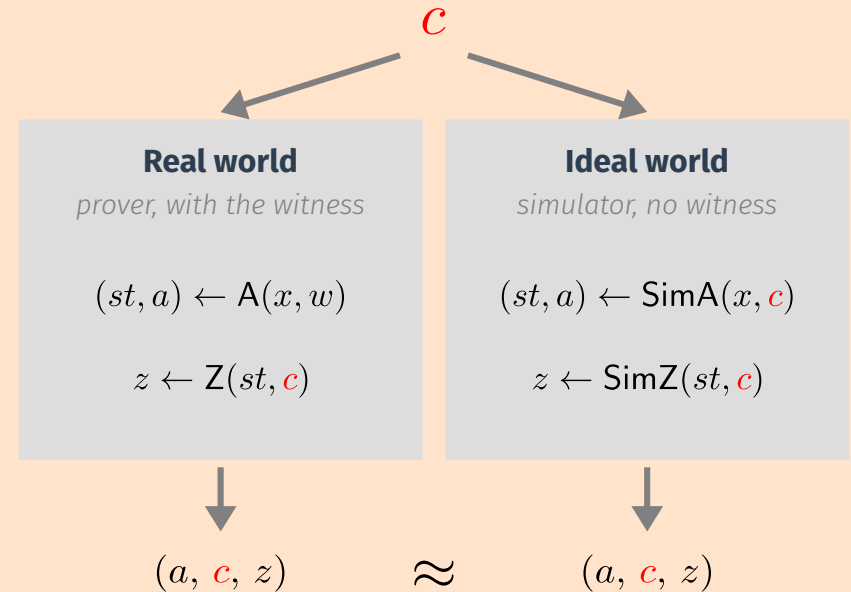


$\text{Ext}((a, c, z), (a, c', z')) \rightarrow w$

Two accepting transcripts with the same a and $c \neq c'$ give a witness

Special honest-verifier ZK

the same challenge in both worlds



SimA needs the challenge **in advance**

Recap: CDS OR-Composition for Σ -Protocols



$P(x^A, x^B, w^A)$

Statement $x^A \vee x^B$, each with a 2-special-sound Σ -protocol
The prover knows a witness w^A for A only



$V(x^A, x^B)$

Simulate B: $c^B \leftarrow \mathcal{C}$, $(a^B, z^B) \leftarrow \text{Sim}(x^B, c^B)$

Real A: $(st^A, a^A) \leftarrow A(x^A, w^A)$

a^A, a^B

red: fixed by the prover before it sees the challenge

c

Challenge: $c \leftarrow \mathcal{C}$

Complete the shares: $c^A := c \oplus c^B$

Answer A honestly: $z^A \leftarrow Z(st^A, c^A)$

c^A, c^B, z^A, z^B

Accept iff $c = c^A \oplus c^B$ and

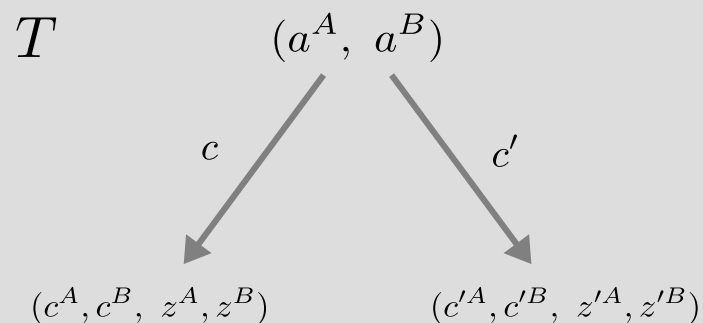
$V(x^j, a^j, c^j, z^j) = 1$ for $j \in \{A, B\}$

Hides the branch: simulated and real transcripts look the same, and each share alone is uniform

2-special sound: two accepting transcripts with $c \neq c'$ differ in c^A or in $c^B \Rightarrow$ extract w^A or w^B

Why CDS Stays 2-Special Sound

Two accepting transcripts: a tree T



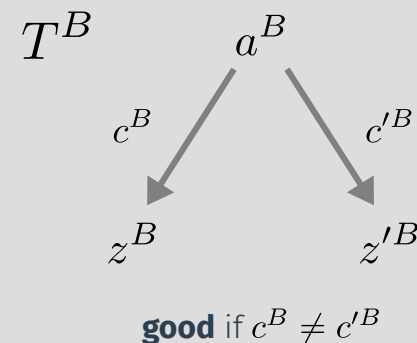
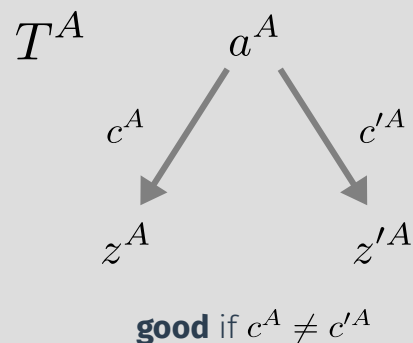
The verifier checked the shares:

$$c = c^A \oplus c^B, \quad c' = c'^A \oplus c'^B$$

Since $c \neq c'$, the shares differ in **at least one** branch:

$$c^A \neq c'^A \quad \text{or} \quad c^B \neq c'^B$$

T decomposes into T^A and T^B



Central observation: at least one of T^A, T^B is a good tree, so its extractor outputs w^A or w^B

Recap: Trapdoor Commitments from Σ -Protocols

key = x (in the CRS), trapdoor = w , **message = challenge**

Commit = simulate

$\text{Com}(x, m): (a, z) \leftarrow \text{Sim}(x, m), \text{com} = a, \text{open} = z$

Ver: accept iff $V(x, a, m, z) = 1$

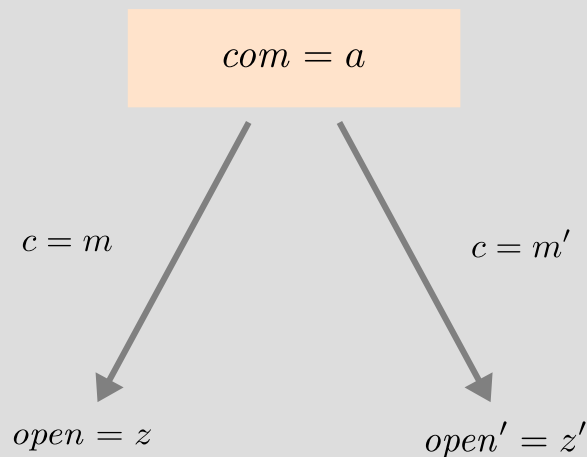
With the trapdoor: equivocate

$(st, a) \leftarrow A(x, w)$, then open to **any** m with the honest response $z \leftarrow Z(st, m)$

Without the trapdoor: binding

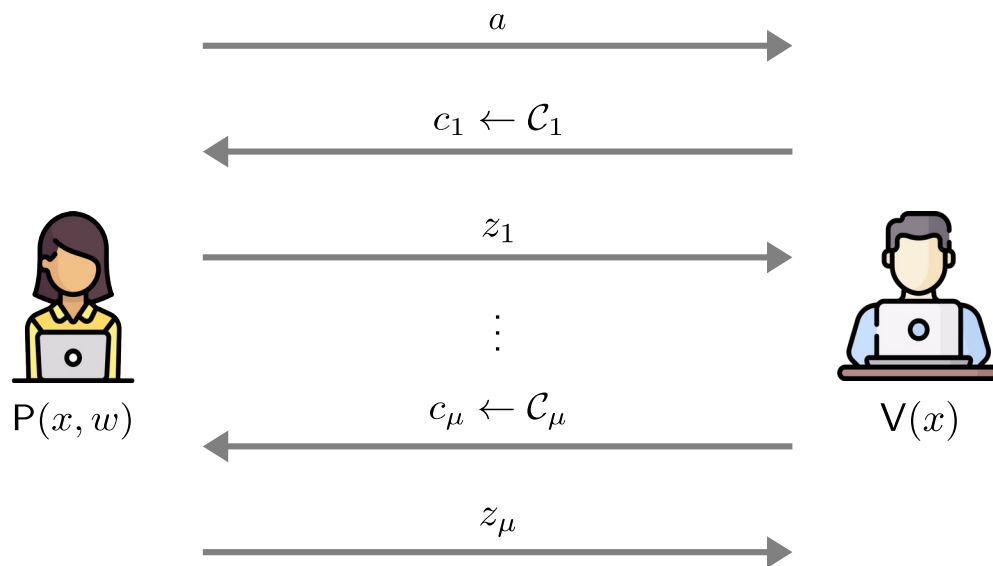
Two openings $(m, z), (m', z')$ of the same a form a 2-tree $\Rightarrow$ 2-special soundness extracts w , contradicting the hardness of R

Two openings = two branches



*with w : both branches answered honestly
without w : the two branches reveal w*

Multi-Round Public-Coin Proofs



μ challenge rounds; the prover speaks first and last

$(2\mu + 1)$ -move transcript

$$(x, a, c_1, z_1, \dots, c_\mu, z_\mu)$$

Stateful prover (A, Z)

$$(st_1, a) \leftarrow A(x, w)$$

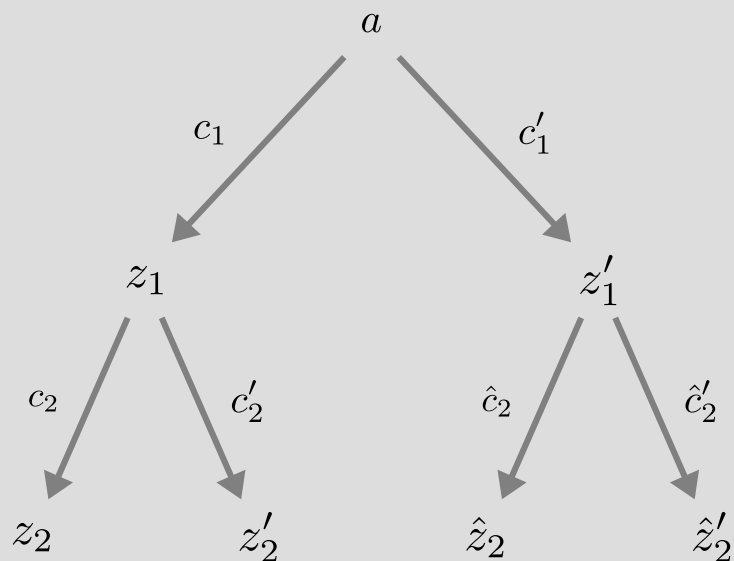
$$(st_{i+1}, z_i) \leftarrow Z(st_i, c_i)$$

Examples

- MPC-in-the-head (KKW18), $\mu = 2$
- Plonk, $\mu = 5$
- Bulletproofs (range proof), $\mu = 4 + \lceil \log(\ell d) \rceil$
- Compressed Σ -protocols, $\mu = \lceil \log(n + 1) \rceil + 1$
 ℓ : number of commitments, d : bit length, n : number of generators

Soundness: Trees of Transcripts

Tree of accepting transcripts



*a (2,2)-tree: two branches per round,
four accepting transcripts*

$(k_1, \dots, k_\mu)$ -special soundness

An extractor computes a witness from any accepting $\vec{k}$ -tree: k_i branches at round i .

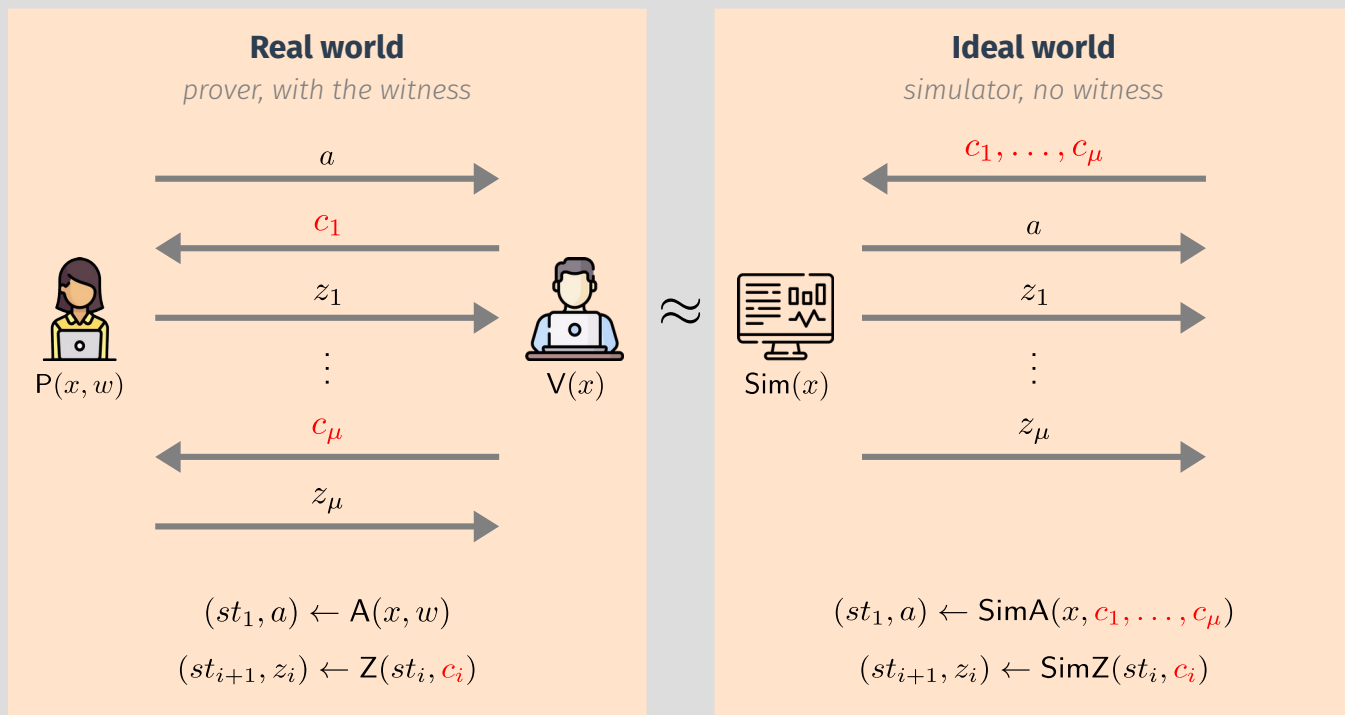
Σ -protocols: $\mu = 1, k_1 = 2$, the 2-tree from the recap

Knowledge soundness via rewinding / tree building [AFK23]

$$\text{Fiat-Shamir knowledge error} \approx (Q + 1) \sum_i \frac{k_i - 1}{|C_i|}$$

What About ZK? A First Attempt

Special honest-verifier ZK for multi-round proofs



Issue

- In the ideal world, **all** challenges come first
- Not sufficient for our applications
 - CDS proof of partial knowledge
 - Trapdoor commitments

First Attempt: Multi-Round CDS from SHVZK



$P(x^A, x^B, w^A)$

Statement $x^A \vee x^B$, each with a multi-round SHVZK proof

The prover knows a witness w^A for A only



$V(x^A, x^B)$

Simulate B: fix $c_1^B, \dots, c_\mu^B$, $(st_1^B, a^B) \leftarrow \text{SimA}(x^B, c_1^B, \dots, c_\mu^B)$

Real A: $(st_1^A, a^A) \leftarrow A(x^A, w^A)$

a^A, a^B



red: fixed by the simulator
before the first message

c_i

Every round i : $c_i \leftarrow \mathcal{C}_i$

Complete the shares: $c_i^A := c_i \oplus c_i^B$

Answer: $z_i^A \leftarrow Z(st_i^A, c_i^A)$, $z_i^B \leftarrow \text{SimZ}(st_i^B, c_i^B)$

$c_i^A, c_i^B, z_i^A, z_i^B$

Accept iff $c_i = c_i^A \oplus c_i^B$ in every round
and both transcripts verify

Same recipe as CDS: complete, and the simulated branch stays hidden

But: B's challenges are all fixed in advance, so the challenge is shared in **every** round. Is it still sound?

Cross Attack on Naive Multi-Round CDS

Typical for multi-round proofs: a prover who knows the challenge of **one** round in advance can cheat

say round 1 for the proof of A and round 2 for the proof of B (e.g. MPC-in-the-head, later in this talk)

Pre-fix one share per round

	A		B
round 1:	$c_1 = \boxed{c_1^A} \oplus c_1^B$		
round 2:	$c_2 = c_2^A \oplus \boxed{c_2^B}$		

cheats in round 1 cheats in round 2

 fixed by the prover before the first message



Cheating prover with no witness

1. Pre-fix c_1^A and c_2^B ; send the first messages a^A, a^B of the two cheating strategies
2. Round 1: set $c_1^B := c_1 \oplus c_1^A$. The proof of A gets its pre-fixed challenge
3. Round 2: set $c_2^A := c_2 \oplus c_2^B$. The proof of B gets its pre-fixed challenge

All checks pass: the verifier **accepts with probability 1**, yet the prover knows **no witness**

SHVZK Is Not Sufficient for Trapdoor Commitments

First attempt: the message fixes all challenges



$\text{Com}(x, m)$: derive $c_1, \dots, c_\mu$ from m , $(st_1, a) \leftarrow \text{SimA}(x, c_1, \dots, c_\mu)$,
 $z_i \leftarrow \text{SimZ}(st_i, c_i)$
 $com = a$, $open = (z_1, \dots, z_\mu)$

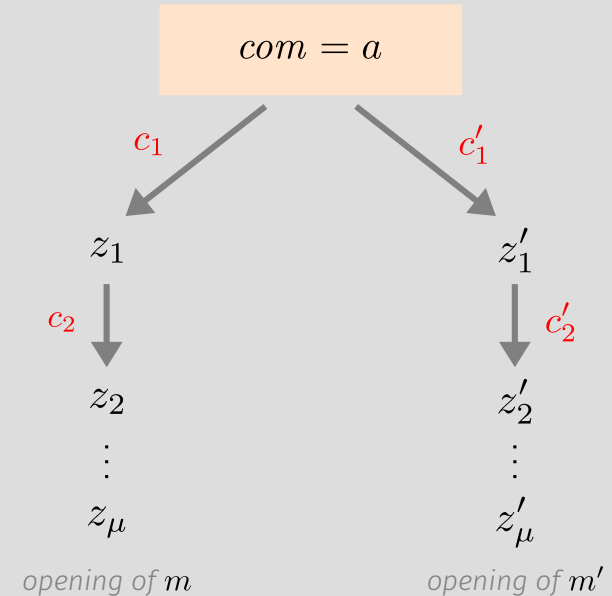
With the trapdoor: equivocate, as before

$(st_1, a) \leftarrow A(x, w)$, then answer the challenges of **any** m with Z

Without the trapdoor: binding fails

- Two openings $m \neq m'$ are two **paths** that split at round 1, not a tree:
- The adversary picks m, m' itself: on each path it knows the later challenges **in advance** and can cheat there, as in the cross attack

Two openings = two paths



*one branch per round after the split;
a tree needs k_i branches at every round*

Roadmap

1

Recap: constructive use of the ZK simulator
for Σ -protocols, and why the naive multi-round extension fails

2

Critical-round SHVZK

one challenge in advance

3

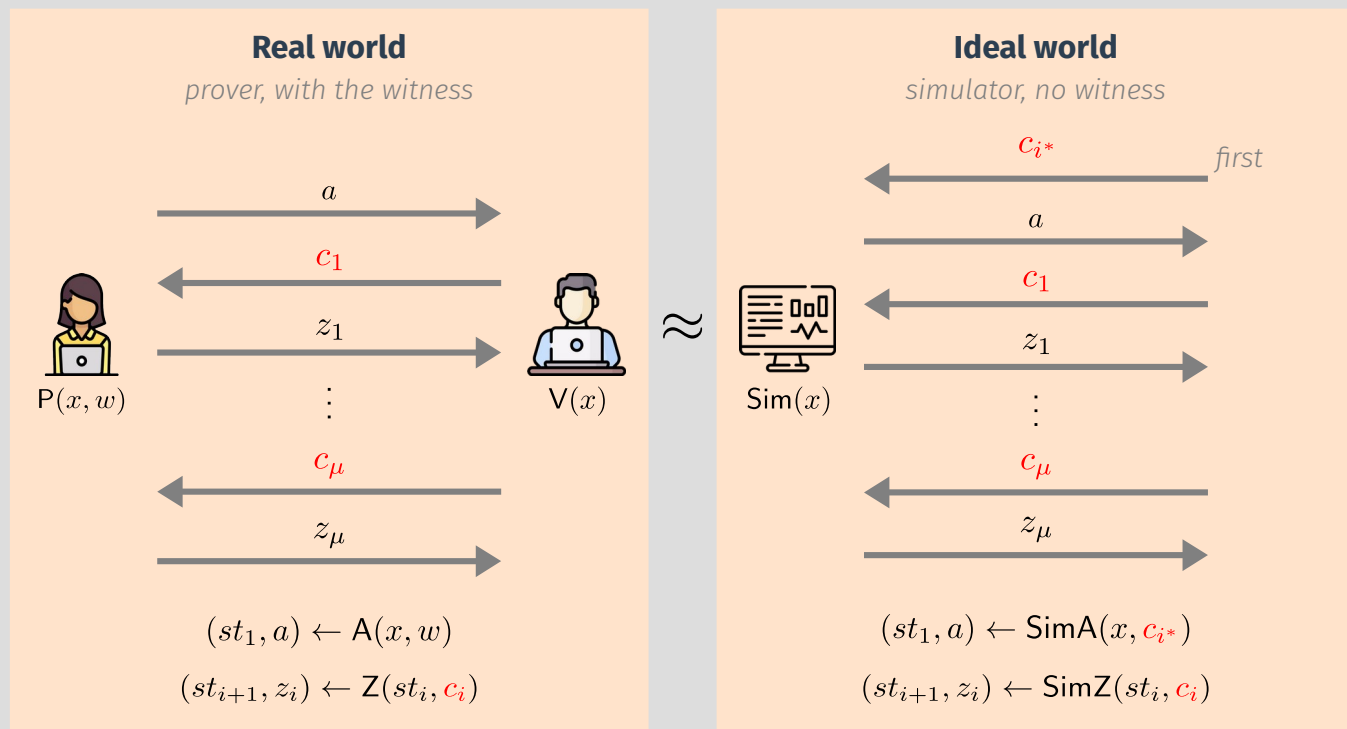
Multi-round proof of partial knowledge
MR-CDS and MR-StH

4

Trapdoor commitments
from multi-round proofs

Critical-Round SHVZK: One Challenge in Advance

Critical-round special honest-verifier ZK (CR-SHVZK)



Idea

- Only **one** challenge comes first: the critical one
- **SimZ** answers online
- Sufficient for our applications
 - CDS proof of partial knowledge
 - Trapdoor commitments
- Inspired by i^* -ZK, defined for Fiat-Shamir [GKK+22, DG23]

Weaker variant: CR-HVZK

$SimA(x) \rightarrow (st_1, a, c_{i^*})$

the simulator picks the critical challenge

Example: KKW MPC-in-the-Head (5-Move)



$P(x, w)$

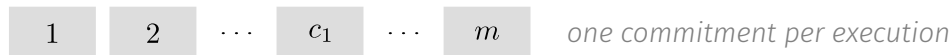
MPC-in-the-head with preprocessing [KKW18], simplified

$c_1 \in [m]$ picks an execution, $c_2 \in [n]$ picks a party

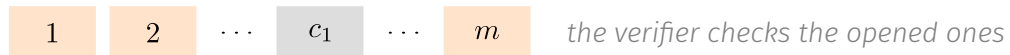


$V(x)$

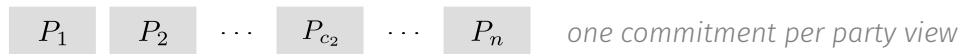
1. Commit to the preprocessed randomness of m MPC executions



2. Open all executions except c_1



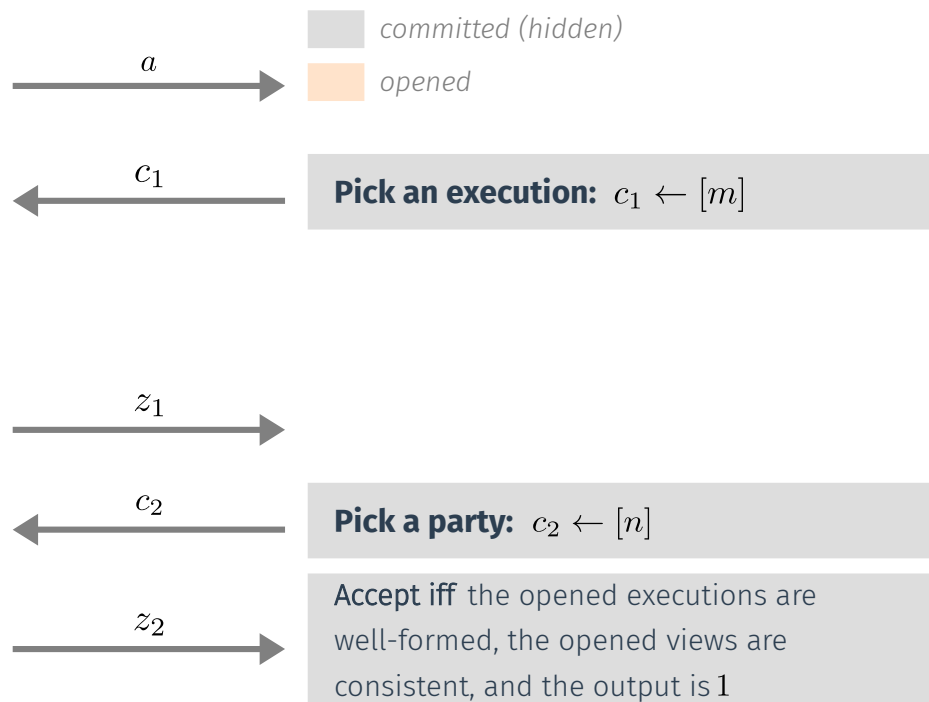
Run the MPC online phase of execution c_1 in the head: parties $P_1, \dots, P_n$, inputs = shares of w , with the unopened randomness. **Commit** to all n views



3. Open all views except that of P_{c_2}



Theorem 1. (2, 2)-special sound and CR-SHVZK at $i^* = 1$ or $i^* = 2$



CR-SHVZK Simulator for KKW at Round 2



$\text{Sim}(x)$

Simulator at round 2: knows c_2 in advance, has no witness
same steps as the honest prover, with one change

1. Commit to the preprocessed randomness of m MPC executions

1 2 ... c_1 ... m as the honest prover

2. Open all executions except c_1

1 2 ... c_1 ... m as the honest prover

► **Run the MPC** online phase of execution c_1 with **random** input shares, and **fake** the messages of P_{c_2} so that the output is 1. **Commit** to all n views

P_1 P_2 ... P_{c_2} ... P_n one faked view

3. Open all views except that of P_{c_2}

P_1 P_2 ... P_{c_2} ... P_n the faked view stays closed

first c_2 committed (hidden)
 a opened
 c_1 differs from the honest prover

Changed: only the online phase of execution c_1 . Random inputs instead of shares of w , and the view of P_{c_2} is produced by the MPC simulator

z_1
 c_2
 z_2

Indistinguishable by all-but-one privacy of the MPC protocol and hiding of the commitment that is never opened

CR-SHVZK Simulator for KKW at Round 1



$\text{Sim}(x)$

Simulator at round 1: knows c_1 in advance, has no witness
same steps as the honest prover, with two changes

- **1. Commit** to the preprocessed randomness; for execution c_1 it is **tampered**

1 2 ... c_1 ... m *one tampered execution*

- **2. Open** all executions except c_1

1 2 ... c_1 ... m *the tampered one stays closed*

- **Run the MPC** online phase of execution c_1 with **random** input shares: the tampering (one correction at the last AND gate) makes the output 1. **Commit** to all n views

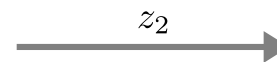
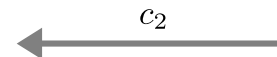
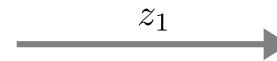
P_1 P_2 ... P_{c_2} ... P_n *every party follows the protocol*

- **3. Open** all views except that of P_{c_2}

P_1 P_2 ... P_{c_2} ... P_n *as the honest prover*



Changed: the correlated randomness of execution c_1 (fixed with the run, in advance), and random inputs instead of shares of w



Indistinguishable: the $n - 1$ opened views pass every check. The tampering can be detected only with all n states of execution c_1 , and one always stays closed

Zoo of Critical Rounds

Protocol	Rounds μ	Critical round	Special soundness	Reference
MPC-in-the-Head (KKW)	2	$i^* \in \{1, 2\}$	(2, 2)	Thm 1
Plonk, 5-round [LPS25]	5	$i^* = 3$	$(3n + 1, 3n + 1, 3, 4n + 21, 6)$	[Lipmaa25, Thm 5]
Bulletproofs: range proof (ARP)	$4 + \lceil \log(\ell d) \rceil$	$i^* = 3$	$(\ell d, \ell + 2, 3, 2, 7, \dots, 7)$	via [DG23]
Bulletproofs: arithmetic circuit (ACS)	$4 + \lceil \log \ell \rceil$	$i^* = 3$	$(\ell, Q + 1, 7, 2, 7, \dots, 7)$	via [DG23]
Compressed Σ -protocols	$\lceil \log(n + 1) \rceil + 1$	$i^* = 1$	$(2, 2, 3, \dots, 3)$	[AC20]

Parameters

Plonk: n gates. ARP: ℓ commitments of d bits. ACS: ℓ multiplication gates, Q linear constraints. Compressed Σ : n group generators.

Roadmap

1

Recap: constructive use of the ZK simulator
for Σ -protocols, and why the naive multi-round extension fails

2

Critical-round SHVZK
one challenge in advance

3

Multi-round proof of partial knowledge
MR-CDS and MR-StH

4

Trapdoor commitments
from multi-round proofs

Multi-Round CDS from CR-SHVZK: the OR Case



$P(x^A, x^B, w^A)$

Statement $x^A \vee x^B$, each with a proof that is CR-SHVZK at round i^*

The prover knows a witness w^A for A only



$V(x^A, x^B)$

Simulate B: fix only $c_{i^*}^B$, $(st_1^B, a^B) \leftarrow \text{SimA}(x^B, c_{i^*}^B)$

Real A: $(st_1^A, a^A) \leftarrow A(x^A, w^A)$

a^A, a^B



red: the only value fixed before the first message

c_i

Rounds $i \neq i^*$: $c_i \leftarrow \mathcal{C}_i$

z_i^A, z_i^B

Same c_i for both: $z_i^A \leftarrow Z(st_i^A, c_i)$, $z_i^B \leftarrow \text{SimZ}(st_i^B, c_i)$

c_{i^*}

Critical round i^* : $c_{i^*} \leftarrow \mathcal{C}_{i^*}$

$c_{i^*}^A, c_{i^*}^B, z_{i^*}^A, z_{i^*}^B$

Complete the share: $c_{i^*}^A := c_{i^*} \oplus c_{i^*}^B$

Answer: $z_{i^*}^A \leftarrow Z(st_{i^*}^A, c_{i^*}^A)$, $z_{i^*}^B \leftarrow \text{SimZ}(st_{i^*}^B, c_{i^*}^B)$

Accept iff $c_{i^*} = c_{i^*}^A \oplus c_{i^*}^B$
and both transcripts verify

The challenge is shared **only** at the critical round; every other round uses the same challenge for both proofs

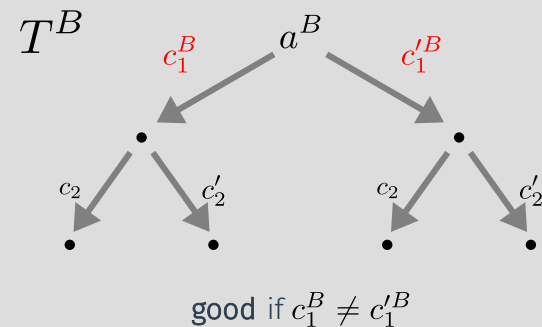
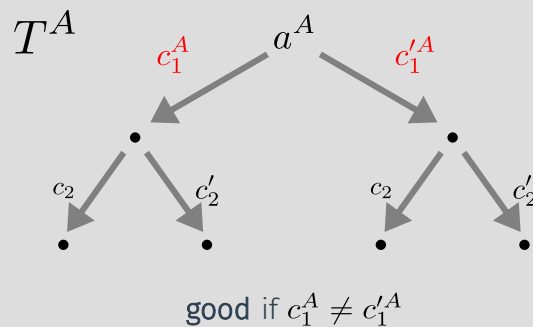
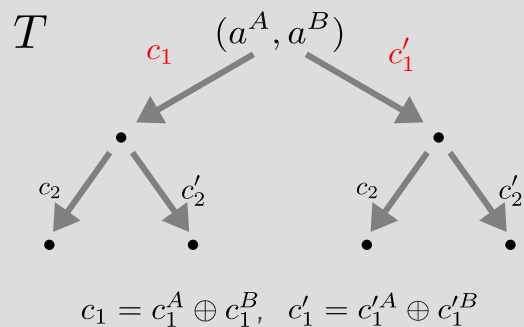
Why This Prevents the Cross Attack

	A	B
round $i \neq i^*$:	$c_i \mapsto c_i$	c_i
round i^* :	$c_{i^*} = \boxed{c_{i^*}^A} \oplus c_{i^*}^B$	

- **Non-critical rounds:** both proofs get the same c_i from the verifier, nothing to pre-fix
- **Critical round:** at most one share can be pre-fixed (red box), as for Σ -protocols

A (2, 2)-tree T decomposes into T^A and T^B

example: two rounds, critical round 1



Central observation: at least one of T^A, T^B is a good (2, 2)-tree, so its extractor outputs w^A or w^B

Theorem (informal): MR-CDS for OR of n Relations

Theorem (informal)

Let $\Pi^1, \dots, \Pi^n$ be proofs for relations $R^1, \dots, R^n$, each

- a $(2\mu + 1)$ -move public-coin proof
- $\vec{k}$ -special sound
- CR-SHVZK at the same critical round i^*

Then the MR-CDS composition is a proof for $R^1 \vee \dots \vee R^n$ that is

- $\implies$
- $\vec{k}'$ -special sound, with $\vec{k}'$ as below
 - CR-SHVZK at i^*

Rounds before: $i < i^*$

$$k'_i = n(k_i - 1) + 1$$

Critical round i^*

$$k'_{i^*} = (k_{i^*} - 1)^n + 1$$

Rounds after: $i > i^*$

$$k'_i = k_i$$

Remarks

- For $k_{i^*} = 2$ and $i^* = 1$: $\vec{k}' = \vec{k}$, so MR-CDS is **closed**
- **Limitation:** for $k_{i^*} > 2$ the knowledge error gains $(k_{i^*} - 1)^n / |\mathcal{C}_{i^*}|$, and the challenge space does not grow with n : only a **constant** number of statements
- The paper proves this for any **monotone access structure**, not just 1-out-of- n OR, with the same special-soundness parameters

Fix: Multi-Round Share-then-Hash

One-line change

$$c_{i*}^j = H(\vec{x}, j, s^j)$$

$s \in S$: the verifier's critical-round challenge; $s^j \in S$: its shares, $s = s^1 \oplus \dots \oplus s^n$

$H : \{0, 1\}^* \rightarrow \mathcal{C}_{i*}$ collision-resistant; S can be much larger than $\mathcal{C}_{i*}$

Intuition

- The secret domain S is decoupled from $\mathcal{C}_{i*}$
- Choose $|S| \gg (k_{i*} - 1)^n$

Effect

- Critical-round branching drops to linear
- The exponential moves into the **numerator** of the knowledge error, where $|S|$ kills it

Analysis

- Proving plain special soundness directly makes the parameters blow up: no meaningful soundness bound
- Instead, analyse in the **predicate special soundness** framework [AAB+24]

MR-StH: the OR Case



$P(x^A, x^B, w^A)$

Share-then-Hash: the critical challenge is the hash of a share, $c_{i*}^j = H(\vec{x}, j, s^j)$

H : collision-resistant hash into $\mathcal{C}_{i*}$; the prover knows w^A only



$V(x^A, x^B)$

Simulate B: fix only the share s^B , $c_{i*}^B := H(\vec{x}, B, s^B)$,
 $(st_1^B, a^B) \leftarrow \text{SimA}(x^B, c_{i*}^B)$

Real A: $(st_1^A, a^A) \leftarrow A(x^A, w^A)$

a^A, a^B



red: the only change
compared to MR-CDS

c_i

Rounds $i \neq i^*$: $c_i \leftarrow \mathcal{C}_i$

z_i^A, z_i^B

Same c_i for both: $z_i^A \leftarrow Z(st_i^A, c_i)$, $z_i^B \leftarrow \text{SimZ}(st_i^B, c_i)$

s

Critical round i^* : $s \leftarrow S$

$s^A, s^B, z_{i*}^A, z_{i*}^B$

Complete the share: $s^A := s \oplus s^B$, $c_{i*}^A := H(\vec{x}, A, s^A)$

Answer: $z_{i*}^A \leftarrow Z(st_{i*}^A, c_{i*}^A)$, $z_{i*}^B \leftarrow \text{SimZ}(st_{i*}^B, c_{i*}^B)$

Accept iff $s = s^A \oplus s^B$ and
both verify with $c_{i*}^j = H(\vec{x}, j, s^j)$

Theorem (informal): MR-StH for OR of n Relations

Theorem (informal)

Let $\Pi^1, \dots, \Pi^n$ be proofs for relations $R^1, \dots, R^n$, and H a hash function, such that

- the proofs are as in the MR-CDS theorem
- H is collision-resistant, with range $\mathcal{C}_{i^*}$

Then the MR-StH composition is a proof for $R^1 \vee \dots \vee R^n$ that is

- CR-SHVZK at i^*

$\implies$ • predicate special sound, with $\vec{k}'$ as below

$$k'_i = n(k_i - 1) + 1 \quad (i < i^*), \quad k'_{i^*} = n(k_{i^*} - 2) + 2, \quad k'_i = k_i \quad (i > i^*)$$

Corollary (Fiat-Shamir, ROM): knowledge error

$$2(Q + 1) \left(\sum_{i \neq i^*} \frac{k'_i - 1}{|\mathcal{C}_i|} + \frac{(k'_{i^*} - 1) \cdot 2^n \cdot (k_{i^*} - 1)^n}{|S|} \right)$$

Remarks

- **Polynomially many statements:** the critical-round branching is linear in n , and a large $|S|$ absorbs the exponential term
- The paper proves this for any **monotone access structure**; the analysis uses predicate special soundness [AAB+24]

Comparison

Scheme	Underlying protocol			Composed protocol				Assumptions
	Rounds	Soundness	ZK	Rounds	Soundness	ZK	Composition	
CDS94	3	2-SS	(S)HVZK	3	2-SS	(S)HVZK	MAS	–
FGQ+23	$2\mu + 1$	RBRS	HVZK	1	CS	HVZK	1-out-of- n	NPROM, CRS
Speed-Stacking	$2\mu + 1$	CS	EHVZK	$2\mu + 1$	CS	EHVZK	t -out-of- n	NIPBC (CRS)
ABO+24	$2\mu + 1$	$\vec{k}$ -SS	HVZK	$2\mu + 1$	$\vec{k}$ -SS	SHVCZK	mNC ¹	DualCom
MR-CDS (ours)	$2\mu + 1$	$\vec{k}$ -SS	CR-(S)HVZK	$2\mu + 1$	$\vec{k}'$ -SS	CR-(S)HVZK	MAS (const. n)	–
MR-StH (ours)	$2\mu + 1$	$\vec{k}$ -SS	CR-(S)HVZK	$2\mu + 1$	$(\vec{k}', \Phi)$ -PSS	CR-(S)HVZK	MAS	CRH

From Table 1 of the paper. **SS**: special soundness, **RBRS**: round-by-round soundness, **CS**: computational soundness, **PSS**: predicate special soundness.
MAS: monotone access structure; efficient whenever it has a polynomial-size monotone span program (**MSP**), e.g. thresholds and AND/OR formulas.
EHVZK: extended honest-verifier ZK, where part of the transcript is simulated independently of the statement. **mNC¹**: polynomial-size monotone formulas.
DualCom: dual-mode commitment (binding or equivocal key). **NIPBC**: non-interactive partially-binding commitment (binding only at hidden positions).

Roadmap

1

Recap: constructive use of the ZK simulator
for Σ -protocols, and why the naive multi-round extension fails

2

Critical-round SHVZK
one challenge in advance

3

Multi-round proof of partial knowledge
MR-CDS and MR-StH

4

Trapdoor commitments
from multi-round proofs

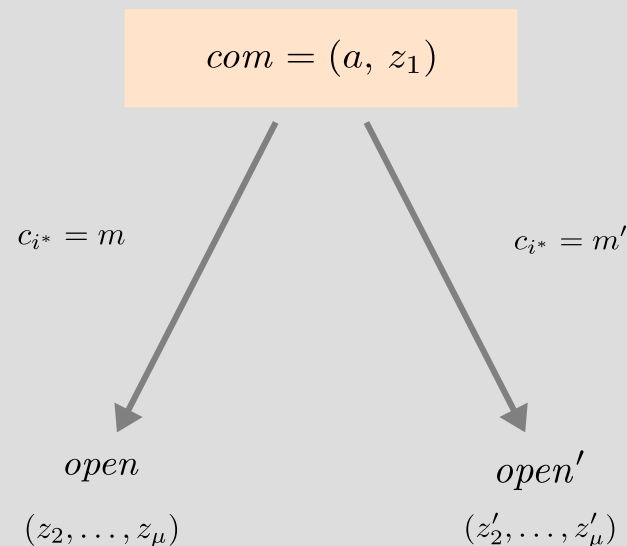
Trapdoor Commitment from a Critical Round

Message = critical challenge, $\mathcal{M} = \mathcal{C}_{i^*}$

$$c_i := \begin{cases} H_i(x, a, z_1, \dots, z_{i-1}) & i < i^* \\ m & i = i^* \\ H_i(x, a, m, z_1, \dots, z_{i-1}) & i > i^* \end{cases}$$

- $\text{Com}(x, m)$: $(st_1, a) \leftarrow \text{SimA}(x, m)$, $z_i \leftarrow \text{SimZ}$; $com = (a, z_1, \dots, z_{i^*-1})$, $open = (z_{i^*}, \dots, z_\mu)$
- $\text{TCom}(w, x)$: honest prover up to round $i^* - 1$
- $\text{Equiv}(st_{i^*}, m)$: continue honestly with $c_{i^*} = m$. **No RO programming** to equivocate
- Ver : recompute c_i , run V

Two openings = two branches



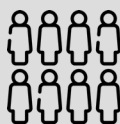
example with critical round 2;
the trapdoor answers both branches honestly

Summary



Critical-round SHVZK

The simulator needs only **one** challenge in advance. Satisfied by MPC-in-the-head, Plonk, Bulletproofs, compressed Σ -protocols



Multi-round proof of partial knowledge

Share only the critical challenge. **MR-CDS**: no extra assumptions, constant number of statements. **MR-StH**: polynomially many statements, from a collision-resistant hash



Trapdoor commitments from multi-round proofs

The message is the critical challenge. Equivocation without programming the random oracle

Sibling work

Critical-Round Special Soundness for Multi-Round Proofs

ePrint 2026/1679

Critical-round special soundness, the soundness-side counterpart, with applications to **verifiable witness sharing** and offline-extractable trapdoor commitments

Thanks!

ePrint 2024/1766

eprint.iacr.org/2024/1766



Backup: Monotone Access Structures

Monotone access structure (MAS)

A family $\Gamma \subseteq 2^{[n]}$ of **qualified** sets that is closed under supersets:

$$A \in \Gamma \text{ and } A \subseteq B \implies B \in \Gamma$$

examples: 1-out-of- n (OR), t -out-of- n (threshold), monotone formulas

Partial knowledge for Γ

$$R_\Gamma(\vec{x}, \vec{w}) = 1 \iff \exists A \in \Gamma \ \forall j \in A : R^j(x^j, w^j) = 1$$

the prover knows witnesses for a qualified set of the n statements

Secret sharing for the dual access structure

$\Gamma^* = \{A : \bar{A} \notin \Gamma\}$, semi-smooth perfect sharing with Share, Rec, CheckShares, Complete

exists for every monotone span program [CDM00]

Key fact (Prop. 5): a set hitting every $B \in \Gamma^*$ is in Γ

Backup: Full MR-CDS Construction



$P(\{x^j\}_{j \in [n]}, \{w^j\}_{j \in A})$

MR-CDS: the share is the critical challenge, $c_{i^*}^j = s^j$

(MR-StH, later: $c_{i^*}^j = H(\Gamma, \vec{x}, j, s^j)$)



$V(\{x^j\}_{j \in [n]})$

Simulate $j \in \bar{A}$: $\{s^j\}_{j \in \bar{A}} \leftarrow D_{\bar{A}}, c_{i^*}^j := s^j, (st_1^j, a^j) \leftarrow \text{SimA}^j(x^j, c_{i^*}^j)$
Real $j \in A$: $(st_1^j, a^j) \leftarrow A^j(x^j, w^j)$

$\{a^j\}_{j \in [n]}$

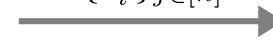


c_i



Same c_i for all: $z_i^j \leftarrow \text{SimZ}^j(st_i^j, c_i) (j \in \bar{A}), z_i^j \leftarrow Z^j(st_i^j, c_i) (j \in A)$

$\{z_i^j\}_{j \in [n]}$



s



Complete the shares: $\{s^j\}_{j \in A} \leftarrow \text{Complete}_{\Gamma^*}(s, \{s^j\}_{j \in \bar{A}}), c_{i^*}^j := s^j$
 $z_{i^*}^j \leftarrow \text{SimZ}^j(st_{i^*}^j, c_{i^*}^j) (j \in \bar{A}), z_{i^*}^j \leftarrow Z^j(st_{i^*}^j, c_{i^*}^j) (j \in A)$

$\{z_{i^*}^j, s^j\}_{j \in [n]}$



Rounds $i \neq i^*$: $c_i \leftarrow \mathcal{C}_i$

Critical round i^* : $s \leftarrow S$

Accept iff all V^j accept and
 $\text{CheckShares}_{\Gamma^*}(s, \{s^j\}_{j \in [n]}) = 1$

Backup: Why the Exponent, and Why It Is Tight

Where the exponent comes from

- Distinct secrets $s \neq \hat{s}$ only force **some** share to differ
- With $k_{i^*} - 1$ pre-fixed challenges per j , a cheater answers up to $(k_{i^*} - 1)^n$ distinct secrets

3-way example, $k_{i^*} = 3$

The cheating prover fixes

$$c^A, \hat{c}^A, \quad c^B, \hat{c}^B, \quad c^C, \hat{c}^C$$

$$\Rightarrow 2^3 = 8 \text{ answerable } c_{i^*} \Rightarrow k'_{i^*} = 9$$

Knowledge error

- Gains $(k_{i^*} - 1)^n / |S|$ with $S = \mathcal{C}_{i^*}$: **constant n only**
- Unlike parallel repetition, the challenge space does not grow

Rounds before the critical one: $i < i^*$

- Branches may yield different qualified sets $A_1, \dots, A_{k'_i}$
- Pigeonhole on $L_j = \{\ell : j \in A_\ell\}$ gives linear $n(k_i - 1) + 1$ instead of the naive $|\Gamma| \cdot k_i$

Backup: Full MR-StH Construction



$P(\{x^j\}_{j \in [n]}, \{w^j\}_{j \in A})$

MR-StH: hash the share, $c_{i^*}^j = H(\Gamma, \vec{x}, j, s^j)$
the secret domain S is independent of $\mathcal{C}_{i^*}$



$V(\{x^j\}_{j \in [n]})$

Simulate $j \in \bar{A}$: $\{s^j\}_{j \in \bar{A}} \leftarrow D_{\bar{A}}$, $c_{i^*}^j := H(\Gamma, \vec{x}, j, s^j)$,
 $(st_1^j, a^j) \leftarrow \text{SimA}^j(x^j, c_{i^*}^j)$
Real $j \in A$: $(st_1^j, a^j) \leftarrow A^j(x^j, w^j)$

$\{a^j\}_{j \in [n]}$

c_i

Rounds $i \neq i^*$: $c_i \leftarrow \mathcal{C}_i$

$\{z_i^j\}_{j \in [n]}$

Same c_i for all: $z_i^j \leftarrow \text{SimZ}^j(st_i^j, c_i) (j \in \bar{A})$, $z_i^j \leftarrow Z^j(st_i^j, c_i) (j \in A)$

s

Critical round i^* : $s \leftarrow S$

$\{z_{i^*}^j, s^j\}_{j \in [n]}$

Complete the shares: $\{s^j\}_{j \in A} \leftarrow \text{Complete}_{\Gamma^*}(s, \{s^j\}_{j \in \bar{A}})$,
 $c_{i^*}^j := H(\Gamma, \vec{x}, j, s^j)$
 $z_{i^*}^j \leftarrow \text{SimZ}^j(st_{i^*}^j, c_{i^*}^j) (j \in \bar{A})$, $z_{i^*}^j \leftarrow Z^j(st_{i^*}^j, c_{i^*}^j) (j \in A)$

Accept iff all V^j accept on the recomputed $c_{i^*}^j$ and
 $\text{CheckShares}_{\Gamma^*}(s, \{s^j\}_{j \in [n]}) = 1$

Backup: Predicate Special Soundness

The framework [AAB+24]

- Extractor only promised on $\vec{k}'$ -trees satisfying a predicate system Φ
- Generalized challenge predicate $\Phi_{m,\ell}^{\text{chal}}(t_1, \dots, t_{\ell-1}, c_\ell)$ reads the previous **subtrees**
- our extension: a good s_ℓ depends on previous responses

Failure density and knowledge error

- $p_{m,\ell}^{\text{chal}}$: worst-case fraction of bad ℓ -th challenges given a good prefix
- Fiat–Shamir knowledge error [AAB+24]:

$$2(Q+1) \sum_i \max\left(\frac{k'_i - 1}{|\mathcal{C}_i|}, \sum_\ell p_{i,\ell}^{\text{chal}}\right)$$

- Extractor cost $K + Q(K-1)$, $K = \prod_i k'_i$

For MR-StH

- Level- i^* predicate: “ s_ℓ is not reconstructable from already-seen shares of any $B \in \Gamma^*$ ” (eq. (2))
- **Lemma 1:** $\tau \geq n(k_{i^*} - 2) + 2$ passing challenges $\Rightarrow$ some $A \in \Gamma$ has k_{i^*} distinct shares for all $j \in A \Rightarrow$ CRH turns them into k_{i^*} distinct $c_{i^*}^j$
- **Lemma 2:** bad set $\subseteq \bigcup_{B \in \Gamma^*} \text{Rec}_{\Gamma^*}(\cdot)$, size $\leq \sum_B \prod_{j \in B} |S_{\ell-1}^j|$

(Backup slide 40 has Lemma 1's counting.)

References

- | | | | |
|-----------|--|------------|---|
| [CDS94] | Cramer, Damgård, Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. CRYPTO '94 | [LPS25] | Lipmaa, Parisella, Siim. On knowledge-soundness of Plonk in ROM from falsifiable assumptions. CRYPTO 2025 |
| [CDM00] | Cramer, Damgård, MacKenzie. Efficient zero-knowledge proofs of knowledge without intractability assumptions. PKC 2000 | [Lipmaa25] | Lipmaa. Plonk is simulation extractable in ROM under falsifiable assumptions. TCC 2025 |
| [AABOR20] | Abe, Ambrona, Bogdanov, Ohkubo, Rosen. Non-interactive composition of sigma-protocols via share-then-hash. ASIACRYPT 2020 | [DG23] | Dao, Grubbs. Spartan and Bulletproofs are simulation-extractable (for free!). EUROCRYPT 2023 |
| [AFK23] | Attema, Fehr, Klooß. Fiat-Shamir transformation of multi-round interactive proofs. J. Cryptology 2023 | [GKK+22] | Ganesh, Khoshakhlagh, Kohlweiss, Nitulescu, Zajac. What makes Fiat-Shamir zkSNARKs (updatable SRS) simulation extractable? SCN 2022 |
| [AFR23] | Attema, Fehr, Resch. Generalized special-sound interactive proofs and their knowledge soundness. TCC 2023 | [AC20] | Attema, Cramer. Compressed Σ -protocol theory and practical application to plug & play secure algorithmics. CRYPTO 2020 |
| [AAB+24] | Aardal, Aranha, Boudgoust, Kolby, Takahashi. Aggregating Falcon signatures with LaBRADOR. CRYPTO 2024 | [HS20] | Haque, Scafuro. Threshold ring signatures: new definitions and post-quantum security. PKC 2020 |
| [KKW18] | Katz, Kolesnikov, Wang. Improved non-interactive zero knowledge with applications to post-quantum signatures. ACM CCS 2018 | | |