ZKProof6 Proposal

On the Security of Nova Recursive Proof System

2024.05.24

Hanyang University

Hyeonbum Lee, Jae Hong Seo

HANYANG UNIVERSITY
SEOUL, KOREA

ZKPROOF

Contents

1. IVC and Nova

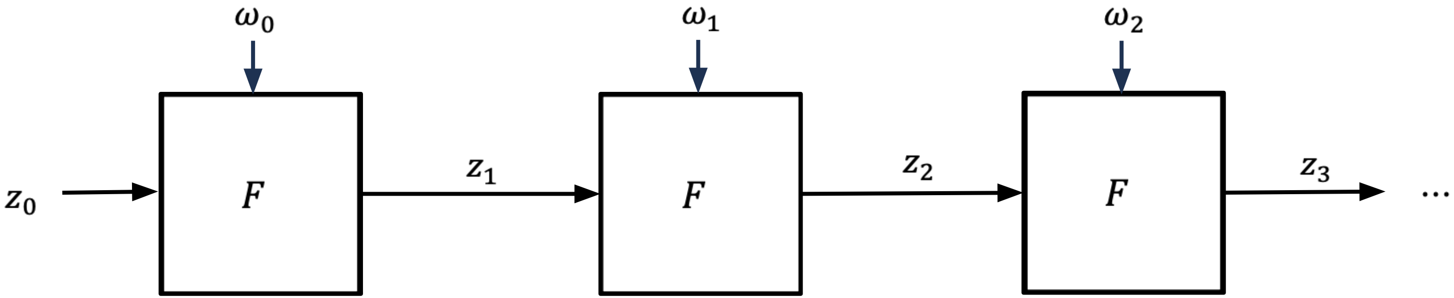
Definition : IVC Scheme

IVC scheme (G, K, P, V)

- Parameter Gen: $G(1^\lambda) \to pp$
- Key Gen: $K(pp, F) \to (pk, vk)$
- IVC Prover: $P(pk, i, z_0, z_i; z_{i-1}, \omega_{i-1}, \Pi_{i-1}) \to \Pi_i$
- IVC Verifier: $V(vk, i, z_0, z_i, \Pi_i) \to 0/1$

IVC proof Π_i guarantees

1. $F(z_{i-1}, \omega_{i-1}) = z_i$
2. $NARK.V(\Pi_{i-1}) = 1$



Folding Scheme: Aggregating Proofs

$\pi_1 : (u_1, w_1) \in R$

$\pi_2 : (U_1, U_1) \in R$

$\xrightarrow{Folding}$

$\Pi : (U, W) \in R$

Π implies $(u_1, w_1) \in R$ and $(U_1, U_1) \in R$

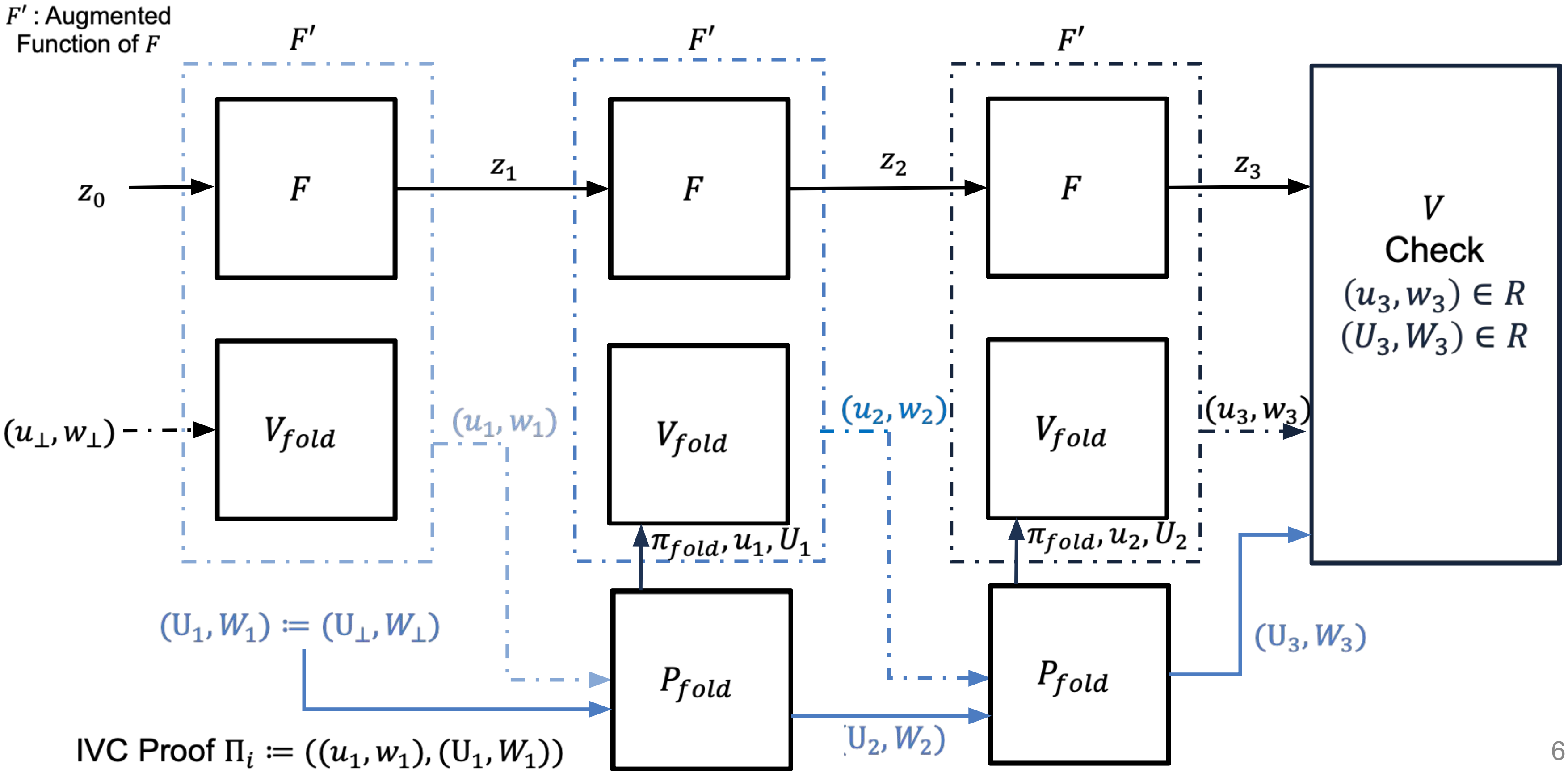
$$\begin{matrix} \pi_1 : (u_1, w_1) \\ \pi_2 : (U_1, U_1) \end{matrix} \longrightarrow \boxed{P_{fold}} \longrightarrow \begin{matrix} \Pi = (U, W), \\ \pi_{fold} \end{matrix}$$

$$\begin{matrix} u_1, U_1, \\ \pi_{fold} \end{matrix} \longrightarrow \boxed{V_{fold}} \longrightarrow U$$

Verify π_1 and π_2 using folding scheme

$V(\pi_1) + V(\pi_2) \Rightarrow V(\pi)$

Nova: Recursive Proof Composition with Folding Scheme



IVC Proof $\Pi_i := ((u_1, w_1), (\mathrm{U}_1, W_1))$

Definition : IVC completeness

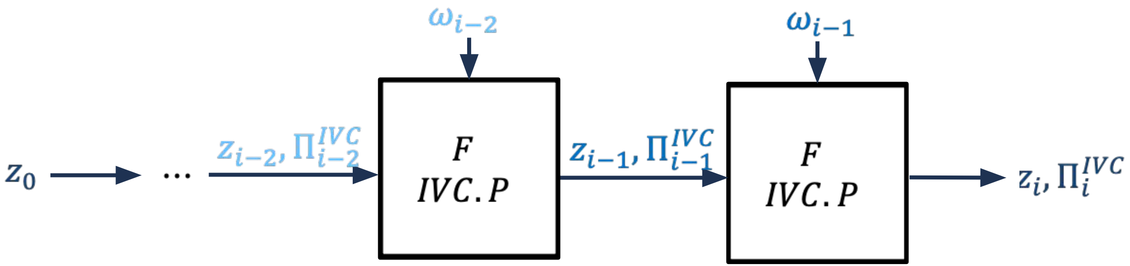
Given IVC scheme (G, K, P, V),

Let $z_i = F(z_{i-1}, \omega_{i-1})$, $V(vk, i-1, z_0, z_{i-1}, \Pi_{i-1}) = 1$, and $\Pi_i \leftarrow P(pk, i, z_0, z_i; z_{i-1}, \omega_{i-1}, \Pi_{i-1})$

Completeness

For any constant i, following equation holds:

$$\Pr[V(vk, i, z_0, z_i, \Pi_i) = 1] = 1$$



Definition : IVC Knowledge Soundness (KS)

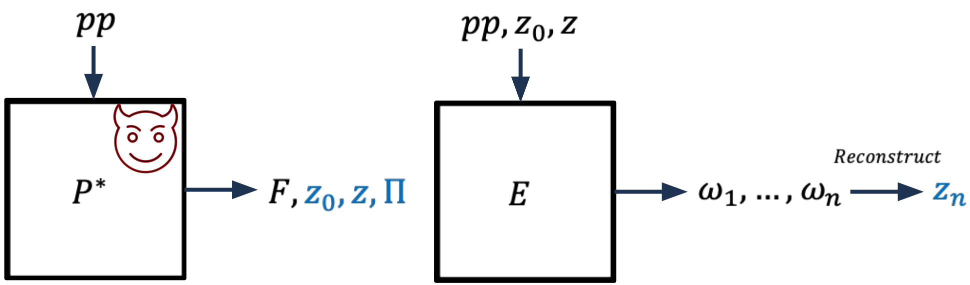
Given IVC scheme (G, K, P, V)

1. Set security parameter λ and constant n. After then set $G(1^\lambda) \rightarrow pp$
2. Adversary P^* outputs execution function F, initial input z_0, final output z, and IVC proof Π
3. Extractor E outputs sequential local inputs $\omega_0, \dots, \omega_{n-1}$
4. Reconstruct z_n from z_0 and $\omega_0, \dots, \omega_{n-1}$ following $F(z_{i-1,}\omega_{i-1}) = z_i$

Knowledge Soundness

For any P^*, there exists PPT E *such that*

$$\Pr[z \neq z_n \wedge V(vk, n, z_0, z, \Pi) = 1] \leq negl(\lambda)$$



The attack succeeds if

1. $z \neq z_n$

2. $V(vk, n, z_0, z, \Pi) = 1$

How large is the constant n?

In Nova, step n is at most poly-logarithm size of security parameter

Ex) security parameter λ bit -> $\mathrm{poly}(\log \lambda)$ steps

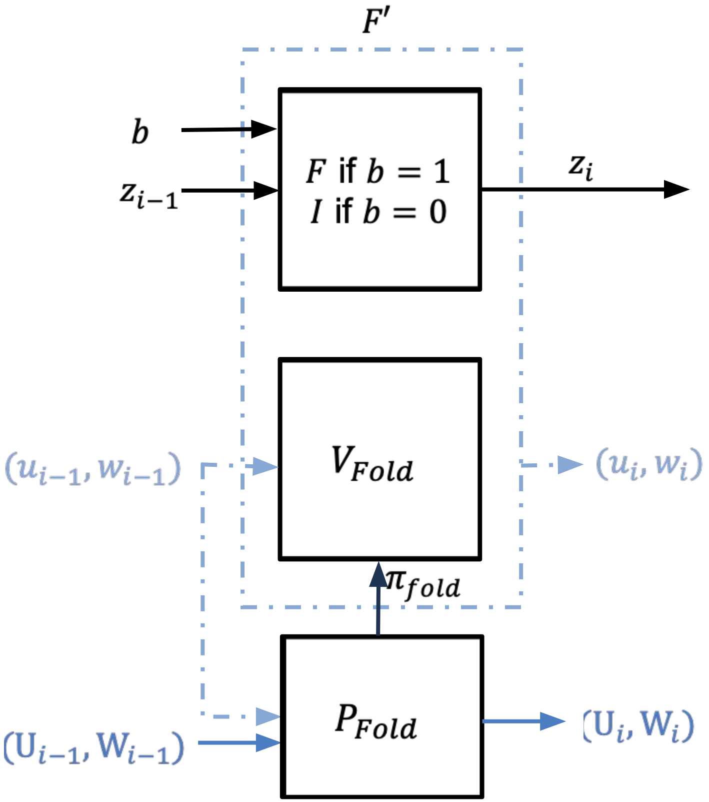
Reason: Blow-up issue for Extraction

The running time of IVC extraction : $2^{O(n)}$

Q: Is the definition of KS sufficient for “sound” IVC?

2. Knowledge Sound but forgeable IVC

Variation of Augmented Execution



IVC prover

Abnormal mode $b = 0$: $z_1 = z_0$

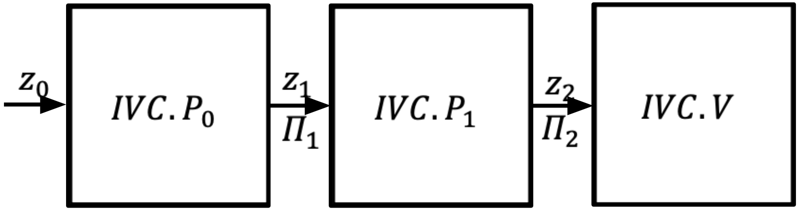
Normal mode $b = 1$: $z_1 = F(z_0)$

- $IVC.P_0$: IVC prover for abnormal mode
- $IVC.P_1$: IVC prover for normal mode

IVC construction using the F'

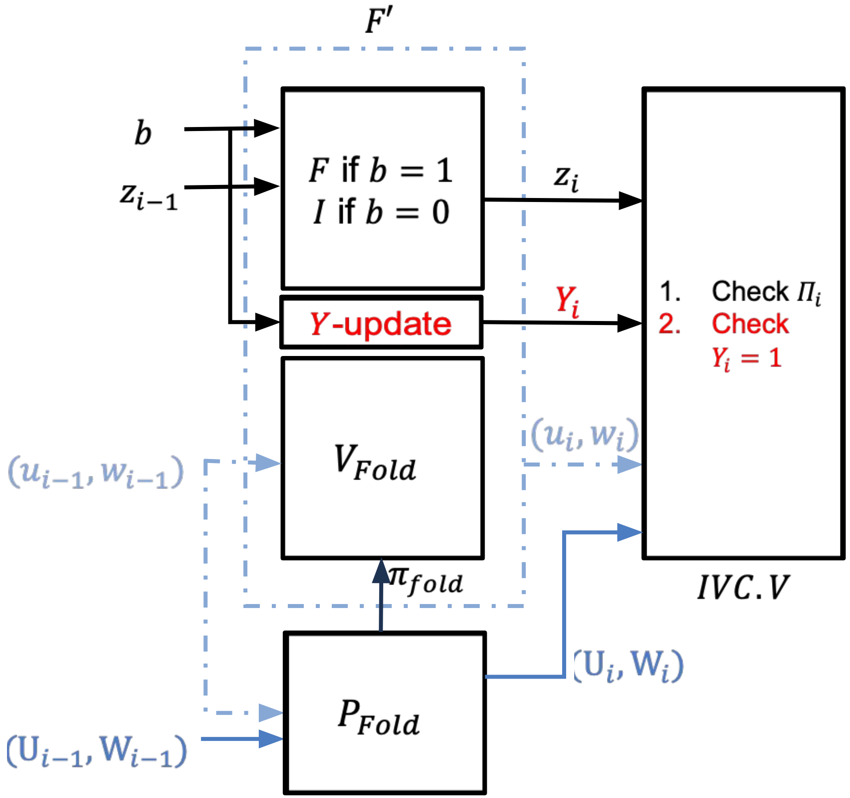
Then, verifier accept both modes, $b = 1/0$

Soundness Issue!



accept Π_2
but $z_2 \neq F^2(z_0)$

Trapdoor Augmented Execution



Add additional variable Y_i

1. $Y_0 := 1$
2. $Y_i = Y_{i-1}^2$ if $b = 1$
3. $Y_i = H(Y_{i-1})$ if $b = 0$

where $H: \mathbb{Z}_p \to \mathbb{Z}_p$ is random oracle

IVC verifier additionally check $Y = 1$

If $IVC.P_1$ is runed for all n steps, $Y_n = 1$

Ephemeral Nova: Nova IVC with the F'

(P_1, V) satisfies completeness

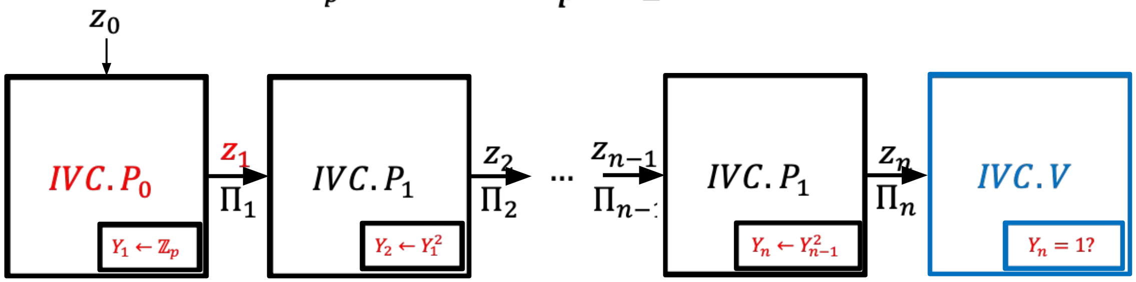
Number Theory Trick

Let p be a $(\lambda + 1)$-bit prime: $2^{\lambda} < p < 2^{\lambda+1}$, and $t < \lambda/2$

Then, $\Pr_{x \leftarrow \mathbb{Z}_p}\left[x^{2^t} = 1\right] \leq 2^{\lambda/2}$

Proof sketch: Degree 2^t polynomial $X^{2^t} - 1$ has at most 2^t zeros. Then,

$$\Pr_{x \leftarrow \mathbb{Z}_p}\left[x^{2^t} = 1\right] \leq \frac{2^t}{p} \leq \frac{2^{\frac{\lambda}{2}}}{2^{\lambda}} = 2^{\frac{\lambda}{2}}$$



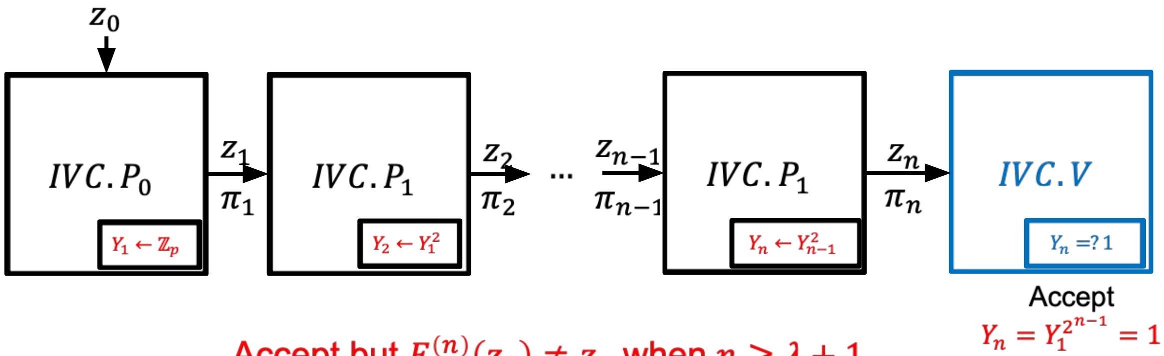
Detectable abnormal mode($b = 0$) within log-previous step, $n = O(\log \lambda) \ll \lambda/2$

Concrete Attack of Ephemeral-Nova

Consider a $(\lambda + 1)$ prime with the form: $p = 2^\lambda + 1$ * In paper, we use the Proth prime, $p = \alpha 2^t + 1$

By Fermat's little theorem, $x^{p-1} = x^{2^\lambda} = 1$ for all nonzero $x \in \mathbb{Z}_p$

If $n > \lambda$, $x^{2^n} = \left(x^{2^\lambda}\right)^{2^{n-\lambda}} = 1^{2^{n-\lambda}} = 1$



Accept but $F^{(n)}(z_0) \neq z_n$ when $n \geq \lambda + 1$

Is Ephemeral-Nova sound?

The Ephemeral-Nova (G, K, P_1, V) satisfies completeness and KS but forgeable in linear steps

Is the KS definition sufficient for non-forgeable IVC? – **No**

Revise definition of KS

1. Set security parameter λ and **polynomial-large n**. After then set $G(1^\lambda) \rightarrow pp$
2. Adversary P^* outputs execution function F, initial input z_0, final output z, and IVC proof Π
3. Extractor E outputs sequential local inputs $\omega_0, \dots, \omega_{n-1}$
4. Reconstruct z_n from z_0 and $\omega_0, \dots, \omega_{n-1}$ following $F(z_{i-1,} \omega_{i-1}) = z_i$

Knowledge Soundness

For any P^*, there exists PPT E *such that*

$$\Pr[z \neq z_n \wedge V(vk, n, z_0, z, \Pi) = 1] \leq negl(\lambda)$$

However… Nova does not satisfy the revised definition in standard model

3. Analysis Models for Group-based Schemes

Blow-up Issue in Nova

Proof of Nova KS

Construct Extractor E using IVC adversary P^*

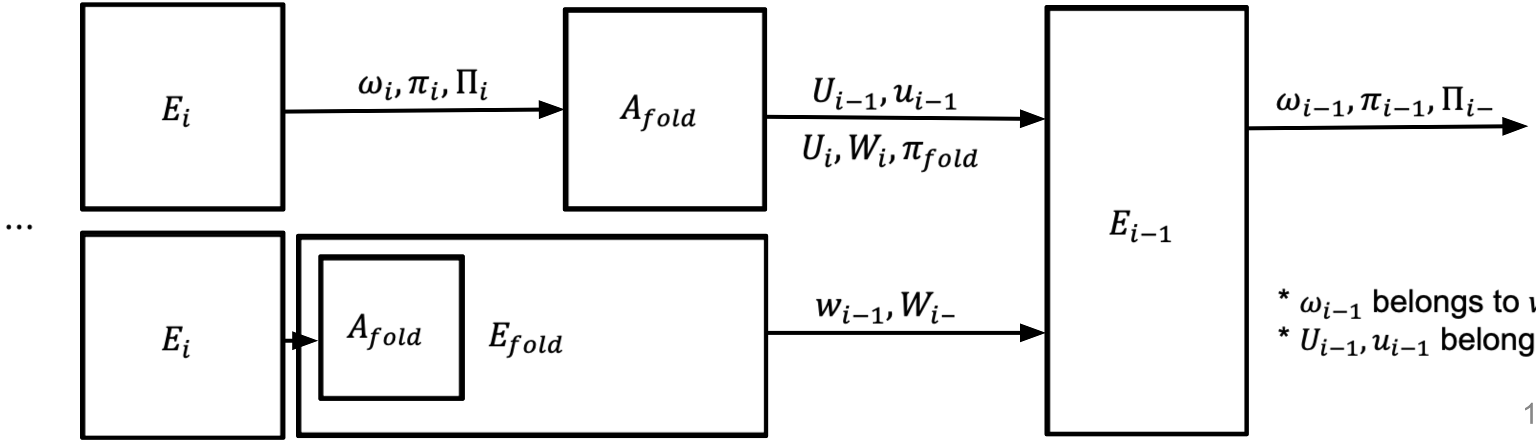
P^*: outputs accepting IVC proof / E: output local inputs $\omega_1, \dots, \omega_n$

E_i: Partial extractor outputs ω_i and i-th proofs $\Pi_i = \big((u_i, w_i), (U_i, W_i)\big)$

A_{fold}: folding adversary / E_{fold}: folding extractor

$$time(E_{i-1}) \geq time\big(A_{fold}\big) + time\big(E_{fold}\big) \geq 2 \cdot time\big(A_{fold}\big) \geq 2 \cdot time(E_i)$$

How to avoid blow-up issue? -> avoid using folding adversary/extractor, Straight-line Extract



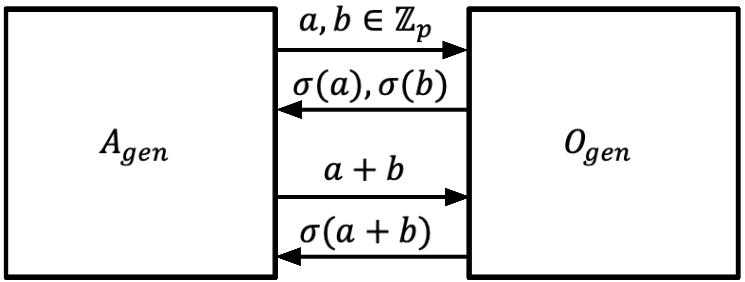
* ω_{i-1} belongs to w_{i-1}
* U_{i-1}, u_{i-1} belong to w_i

Model candidates: GGM and AGM

Generic Group Model(GGM)

An idealized model where all group operations of adversary A_{gen} are carried out by making oracle queries

The adversary A_{gen} records the oracle response for group elements



Model candidates: GGM and AGM

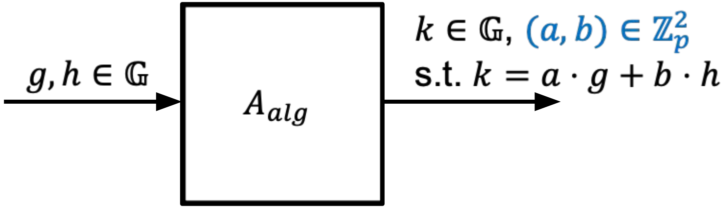
Algebraic algorithm A_{alg}

If A_{alg} outputs group elements $h \in \mathbb{G}$, A_{alg} also outputs a representations $\boldsymbol{x} \in \mathbb{Z}_p^n$ such that $h = \langle \boldsymbol{x}, \boldsymbol{g} \rangle$, where $\boldsymbol{g} \in \mathbb{G}^n$ is given to A_{alg} beforehand.

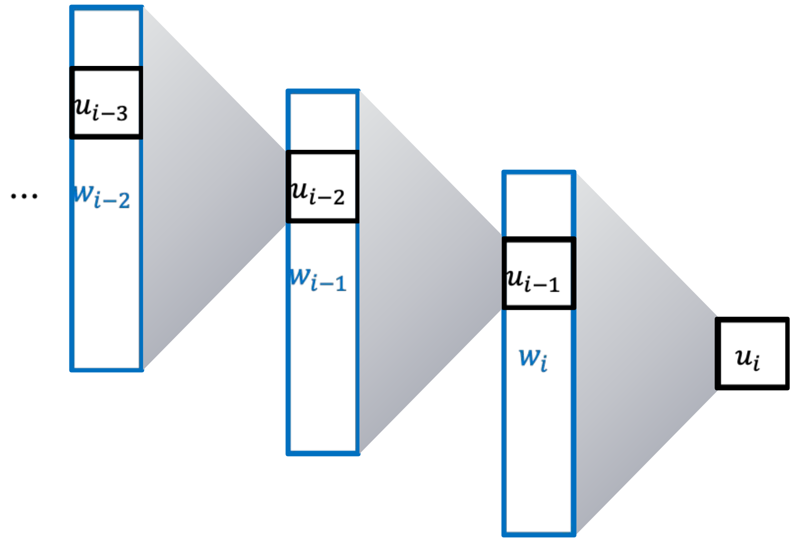
$\mathbb{G}$: cyclic group of order p

Algebraic Group Model

A computational model in which all adversaries are modeled as Algebraic



Structure of Nova and limitation of GGM



u : Pedersen Commitment to witness w, group element in $\mathbb{G}$
w : R1CS witness, representation of u, vector over in $\mathbb{Z}_p$

Extract Process

For $i = n, \dots, 1$

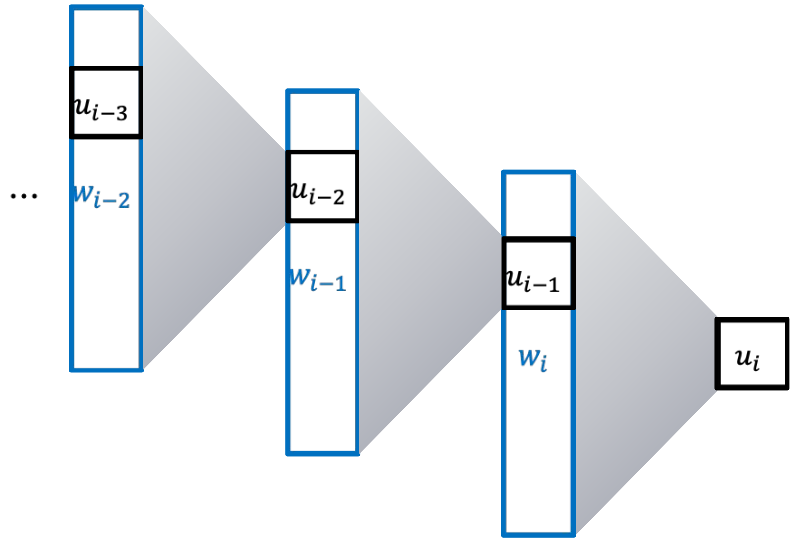
1. Extract witness w_i for instance u_i
2. Retrieve u_{i-1} from w_i

Extract witness w_0 for instance u_0

The group element u_{i-1} is instantiated to a field element in vector w_i

In GGM, hard to describe the instantiation.
Because a group element is like a random bitstring in the view of the adversary

Make Clear the Action of Algebraic Adversary



u : Pedersen Commitment to witness w, group element in $\mathbb{G}$
w : R1CS witness, representation of u, vector over in $\mathbb{Z}_p$

Let A_{alg} output $\Pi_i = (u_i, w_i)$

Explicitly, w_i is not a group element

However, w_i contains group encodable part u_{i-1}

Then, should A_{alg} provide a representation of u_{i-1}?

Our answer is Yes!

Due to R1CS constraints, w_i contains group encodable part u_{i-1} if Π_i is valid proof

4. Zero-Testing Hash Functions

Random Oracle and Schwartz-Zippel Lemma

To instantiate non-interactive Folding Verifier, one needs RO instantiation

Why need RO? => Fiat-Shamir, substitute verifier challenge with RO output

Role of Verifier Challenge: Reduce checking many points to a random point

Ex) Polynomial Check ($f(X) = 0$) => Evaluation Check ($f(r) = 0$)

Schwartz-Zippel Lemma

$f(r) = 0$ for random $r \leftarrow \mathbb{Z}_p$ => $f(X) = 0$ with high probability (error: $\deg(f)/p$)

Is the RO condition necessary?

Zero-Testing Hash Function

Zero-Testing Property

For any PPT adversary cannot find a polynomial $poly \in \mathbb{Z}_p[X]$ of degree $O(\lambda)$ that satisfies $poly\big(Hash(poly)\big) = 0 \ (mod\ p)$

General Zero-Testing(GZT) Property

- $Com: Domain \to C$: binding commitment
- $D: Domain \to \mathbb{Z}_p^{\leq O(\lambda)}[X]$: arbitrary map to polynomial with degree at most $O(\lambda)$

For any PPT adversary cannot find $d \in Domain$ and auxiliary input τ that satisfies $D(d)\big(Hash(C(d), \tau)\big) = 0 \ (mod\ p)$

Theorem

If $Hash$ is RO, then $Hash$ satisfies GZT property

Schnorr's NIZK in the AGM with GZT hash

$$R = \{(G, H; x) \colon H = x \cdot G\}$$

$$P \xrightarrow{\pi = (s, K)} V$$

P:

1. $k \leftarrow \mathbb{Z}_p; K = k \cdot G$
2. $e \leftarrow hash(K, G, H)$
3. $s = k + ex$

V:

1. $e \leftarrow hash(K, G, H)$
2. Check $s \cdot G = K + e \cdot H$

Schnorr's NIZK

Proof

$$x' = \frac{s' - k_1}{e' + k_2} \xleftarrow{e' = hash(K', G, H)} E \xleftarrow[\text{s.t. } k_1 \cdot G + k_2 \cdot H]{\pi' = (s', K'), (k_1, k_2)} A_{alg} \longleftarrow G, H$$

Straight-line Extract from A_{alg}

If $e' + k_2 = 0$, the $hash$ does not satisfy GZT property

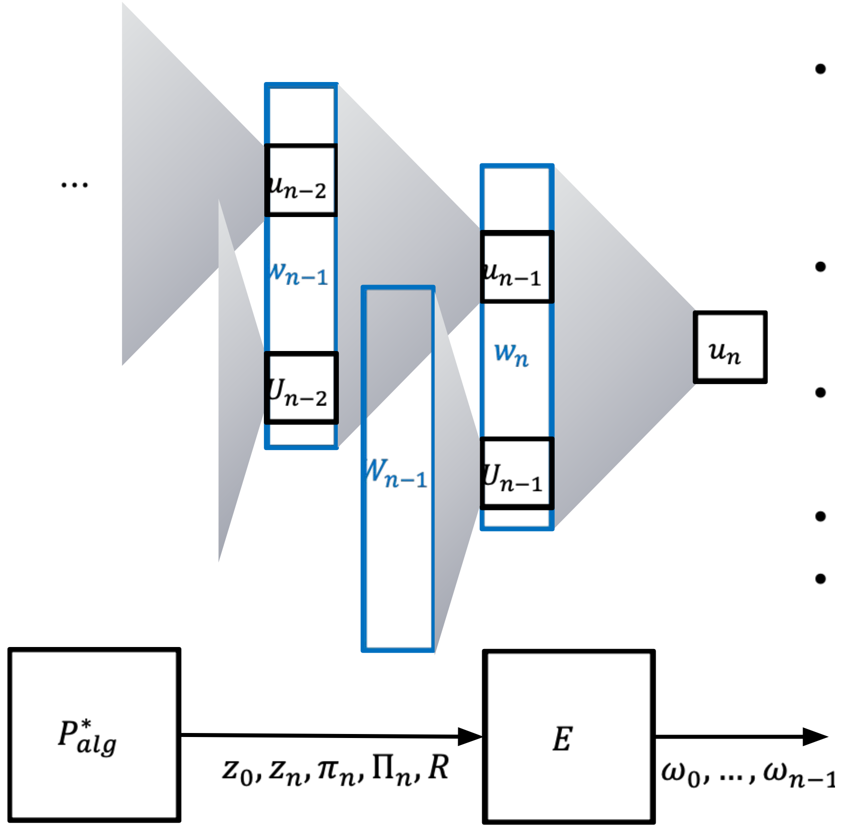
Set $D(k_1, k_2) = X + k_2$, $com(k_1, k_2) = k_1 \cdot G + k_2 \cdot H$, and $\tau = (G, H)$

Then, $D(k_1, k_2)\big(hash(com(k_1, k_2), G, H)\big) = e + k_2 = 0$, the adversary find the zero

In the similar way, NIFS KS can be proven without RO in AGM

5. Nova KS Proof and Conclusion

Construct Extractor in AGM



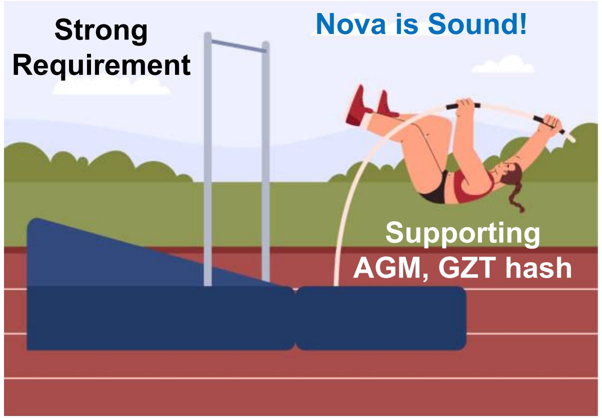
- If IVC adversary P^*_{alg} outputs accepting proof $\Pi_n = \big((U_n, W_n), (u_n, w_n)\big)$ then it also outputs representation set R
- By accepting proof Π_n, can get representations w'_{n-1} and W'_{n-1} of u_{n-1} and U_{n-1} from R
- By the NIFS-KS, w'_{n-1} and W'_{n-1} are indeed witness of u_{n-1} and W_{n-1}
- Using the extraction recursively, get $\Pi_{n-1}, \ldots, \Pi_1$
- Extractor finds $\omega_0, \ldots, \omega_{n-1}$ from Proofs $\Pi_n, \ldots, \Pi_1$

Nova is poly-step KS in AGM

Conclusion

1. Give a forgeable IVC that satisfies KS
   The definition of KS should cover polynomially-large step

2. Prove poly-step KS of Nova in AGM
   Make clear roles of algebraic adversary
   Propose weaker condition for hash: do not rely on RO in AGM



Thank You

ePrint: 2024/232