stackproofs: Private proofs of stack and contract execution using ProtoGalaxy

Liam Eagen[1], Ariel Gabizon[2], Marek Sefranek[3], Patrick Towa[2], and Zachary J. Williamson[2]

[1]Alpen Labs
[2]Aztec Labs
[3]TU Wien

August 8, 2024

Abstract

The goal of this note is to describe and analyze a simplified variant of the zk-SNARK construction used in the Aztec protocol. Taking inspiration from the popular notion of Incrementally Verifiable Computation[Val08] (IVC) we define a related notion of *Repeated Computation with Global state* (RCG). As opposed to IVC, in RCG we assume the computation terminates before proving starts, and in addition to the local transitions some global consistency checks of the whole computation are allowed. However, we require the space efficiency of the prover to be close to that of an IVC prover not required to prove this global consistency. We show how RCG is useful for designing a proof system for a private smart contract system like Aztec.

1 Introduction

Incrementally Verifiable Computation (IVC) [Val08] and its generalization to Proof Carrying Data (PCD) [CT10] are useful tools for constructing space-efficient SNARK provers[BCCT12]. In IVC and PCD we always have an acyclic computation. However code written in almost any programming language *is* cyclic in the sense of often relying on internal calls - we start from a function A, execute some commands, go into a function B, execute its commands, and go back to A. When making a SNARK proof of such an execution, we typically linearize or "flatten" the cycle stemming from the internal call, in one of the following two ways.

1. The monolithic circuit approach - we "inline" all internal calls (as well as loops) into one long program without jumps.

2. The VM approach - assume the code of A, B is written in some prespecified instruction set. The program is executed by initially writing the code of A, B into memory, and loading from memory and executing at each step the appropriate instruction according to a program counter. For example, the call to B is made by changing the counter to that of the first instruction of B. To prove correctness of the execution, all we need is a SNARK for proving correctness of a certain number of steps of a machine with this instruction set, and some initial memory state.

The second approach is more generic, while the first offers more room for optimization, so we'd want to use it in resource-constrained settings, e.g. client-side proving.

However, what if we're in a situation where A and B have already been "SNARKified" separately? Namely, there is a verification key attached to each one, and we are expected to use these keys specifically. This is what happens in the Aztec system.

The Aztec private contract system: Similar to Ethereum - we have contracts; and the contracts have functions. A function in a contract can internally call a different function in the same or a different contract. Moreover, while writing the code for the different functions, we can't predict specifically what function will be internally called by a given contract function. For example, a "send token" function could have an internal call to an "authorize" function. But the call to "authorize" need not be tied to a specific implementation, and consequently verification key - as different token holders are allowed to set their own "authorize" function.

The goal of the Aztec system is to enable constructing zero-knowledge proofs of such contract function executions. For this purpose, a contract is deployed by

1. Computing a verification key for each function of the contract.

2. Adding a commitment to the verification keys of the contract in a global "function tree". More accurately, a leaf of this tree is a hash of the contract address with a Merkle root of a tree whose leaves are the verification keys of that contract's functions.

Dealing with Global state Each contract has a set of notes - which are simply values in a field $\mathbb{F}$. While running, a function can read, add or delete notes belonging to its contract. We can thus think of the notes as global variables shared between the different functions.

Assume all functions in this system return accept or reject. (We can always move the output into the arguments if a function is not of this form.) Here's a natural way to prove the mentioned execution: Put the arguments to B in the public inputs of both the circuits of A and B. Verify the proofs π_A, π_B for A, B; and check via the public inputs the same value was used in both proofs for the arguments of B.

This however, doesn't yet deal with the notes. During execution, note operations happened in a certain order. We can thus assign a *counter* equal to one to the first operation, and increment the counter with each operation. We then need to check, for

example, that if a note was read with a certain counter, it was indeed added with a smaller counter. We can include a description of the note operations peformed by a function in the inputs of its circuit. This description will contain the operation type - $\{\mathsf{add}, \mathsf{read}, \mathsf{del}\}$, the note value, and the counter. The issue is, what if A is reading a note that was added in the internal call to B? Checking the existence of an add operation with smaller counter requires a constraint *between* the inputs of both circuits. And for an execution consisting of more calls, this constraint can involve any two circuits in the call tree.

This brings us to the notion of *Repeated Computation with Global state* (RCG). In RCG we have a transition predicate taking us from one state to the next. We wish to prove we know a sequence of witnesses taking us from a legal initial state to a certain publicly known final state. This might remind the reader of the popular notion of *incrementally verifiable computation* (IVC). There are two differences.

- In RCG we are not interested in "incremental" proofs of one step, only in proofs for a whole sequence of transitions ending in a desired final state.
- In RCG we also have a *final predicate* checking a joint consistency condition between witnesses from all iterations.

One could ask, why not *only* have a final predicate that includes the transition checks? In other words, a monolithic circuit for the whole computation. The point is that in our use case the final predicate is applied to small parts of each iteration's witness - namely the note operations. As a result, the decomposition into a transition and final predicate can facilitate obtaining better prover efficiency, especially in terms of prover space. Roughly, we'll require space sufficient for storing the inputs to the final predicate, in addition to the space required to prove a single transition.

1.1 Related work

Recent work [**?**, **?**] as well as ongoing work [**?**] uses folding schemes[KST21] to break up proving statements about large computation into smaller statements. The objective being reducing prover memory and/or improving prover parallelism. These works, as far as we know, have not formally defined a notion like RCG, and rather use the IVC terminology. However we believe they implicitly use RCG, because of the need to check global constraints between the different chunks.

2 Preliminaries

2.1 Terminology and Conventions

We assume all algorithms described receive as an implicit parameter the security parameter λ. Similarly, all integer parameters in the paper are implicitly functions of λ, and of size at most $\mathsf{poly}(\lambda)$ unless explicitly stated otherwise.

Whenever we use the term *efficient*, we mean an algorithm running in time $\mathsf{poly}(\lambda)$. Furthermore, we assume an *object generator* $\mathcal{O}$ that is run with input λ before all protocols, and returns all fields and groups used. Specifically, in our protocol $\mathcal{O}(\lambda) = (\mathbb{F}, \mathbb{G}, g)$ where

- $\mathbb{F}$ is a field of **prime** size $r = \lambda^{\omega(1)}$.
- $\mathbb{G}$ is a group of size r.
- g is a uniformly chosen generator of $\mathbb{G}$.

We usually let the λ parameter be implicit, e.g. write $\mathbb{F}$ instead of $\mathbb{F}(\lambda)$. We denote by $\mathbb{F}_{<d}[X]$ the set of univariate polynomials over $\mathbb{F}$ of degree smaller than d. We write $\mathbb{G}$ additively.

We often denote by $[n]$ the integers $\{1, \ldots, n\}$. We use the acronym e.w.p. for "except with probability"; i.e. e.w.p. γ means with probability *at least* $1 - \gamma$.

Representing $\mathbb{G}$ Assume an injective function $R : \mathbb{G} \to \mathbb{F}^2$. Whenever we discuss $a \in \mathbb{G}$ we assume it is represented as $R(a)$. When we say for $b \in \mathbb{F}^2$ that $b \in \mathbb{G}$ we mean that there exists $a \in \mathbb{G}$ with $R(a) = b$.

3 The execution model:

We present a formal framework that will be convenient for our proof system of what it means to prove an execution where functions can call each other, and there is global state. For this, we first introduce record operations which is our specific notion of operating on a global state.

3.1 Record operations

Records are pairs (v, c) - where $\mathsf{v} \in \mathbb{F}$ is the *value*, and $\mathsf{c} \in [M]$ is a *counter*. A *record operation* has one of the following forms:

- $(\mathsf{add}, \mathsf{v}, \mathsf{c})$,
- $(\mathsf{del}, \mathsf{v}, \mathsf{c_v}, \mathsf{c})$,
- $(\mathsf{read}, \mathsf{v}, \mathsf{c_v}, \mathsf{c})$.

Here $\mathsf{v} \in \mathbb{F}$ is a value and $\mathsf{c}, \mathsf{c_v} \in [M]$ are counters. c is interpreted as the counter of the current operation. $\mathsf{c_v}$ is interpreted as the counter of the operation where the note was added in the case of a read or del operation.

We say a sequence $\mathcal{O}$ of record operations of size M is *consistent* if

1. The counter values c are distinct in all elements of $\mathcal{O}$, and as a set equal to $[M]$.
2. The $\mathsf{c_v}$ fields in all del operations $(\mathsf{del}, \mathsf{v}, \mathsf{c_v}, \mathsf{c}) \in \mathcal{O}$ are distinct.

3. If $(\mathsf{v}, \mathsf{read}, \mathsf{c_v}, \mathsf{c}) \in \mathcal{O}$, then $\mathsf{c_v} < \mathsf{c}$ and $(\mathsf{add}, \mathsf{v}, \mathsf{c_v}) \in \mathcal{O}$.

4. If $(\mathsf{v}, \mathsf{del}, \mathsf{c_v}, \mathsf{c}) \in \mathcal{O}$ then $\mathsf{c_v} < \mathsf{c}$ and $(\mathsf{add}, \mathsf{v}, \mathsf{c_v}) \in \mathcal{O}$.

Let V be a set of records. We say $\mathcal{O}$ is *has output* V if:

- $\mathcal{O}$ is consistent.
- $\mathsf{V} = \{(\mathsf{v}, \mathsf{c}) | (\mathsf{add}, \mathsf{v}, \mathsf{c}) \in \mathcal{O} \ \& \ \forall \mathsf{c}' \in [M], (\mathsf{del}, \mathsf{v}, \mathsf{c}, \mathsf{c}') \notin \mathcal{O}\}$. In words, V is the set of notes that were added and not deleted.

3.2 The plonkish relation

Now we introduce a relation describing the individual function executions tailored to make it convenient to later discuss an execution of a sequence functions calling each other. Some choices of constants - like args being of size four, are arbitrary. We require the instance to adhere to a form containing both the record operations and the details of the inner calls (though they will be interpreted as such only in the next section when we discuss valid executions).

We fix a polynomial $G : \mathbb{F}^8 \to \mathbb{F}$, and integers N, n that are implicit parameters in the following definition of the relation $\mathcal{R}_{app}$.

$\mathcal{R}_{app}$ consists of all pairs $(\mathfrak{x}, \mathfrak{w})$ having the form

- $\mathfrak{x} = (\mathsf{f}, \mathsf{args}, \mathsf{c}, \mathsf{f}_1, \mathsf{args}_1, \mathsf{f}_2, \mathsf{args}_2, \mathcal{O})$ where $\mathsf{f}, \mathsf{f}_1, \mathsf{f}_2 \in \mathbb{G}, \mathsf{args} \in \mathbb{F}^4, \mathsf{c} \in \{0, 1, 2\}$;
- $\mathfrak{w} = (\mathsf{w_f}, \omega)$ where
  - $\mathsf{w_f} = (\mathsf{S}_1, \ldots, \mathsf{S}_4, \mathsf{q}_1, \ldots, \mathsf{q}_4)$,where $\mathsf{S}_j \in [|\mathfrak{x}| + N]^{\mathit{n}}, \mathsf{q}_j \in \mathbb{F}^{\mathit{n}}$ for each $j \in [4]$
  - $\omega \in \mathbb{F}^N$

such that

1. Setting $x = (\mathfrak{x}, \omega)$, for all $i \in [\mathit{n}]$

$$G(\mathsf{q}_{1,i}, \ldots, \mathsf{q}_{4,i}, x_{\mathsf{S}_{1,i}}, \ldots, x_{\mathsf{S}_{4,i}}) = 0.$$

2. $\mathsf{f} = \mathsf{cm}(\mathsf{w_f})$.

3.3 Valid execution trees

By an *execution tree of length* n we mean a binary tree T with n vertices, whose nodes are labeled by pairs $(\mathfrak{x}, \mathfrak{w})$. Let F be a set of elements of $\mathbb{G}$. Given such T we say it is a *valid execution of length* n *with function set* F *and output* V if

1. For each $\mathsf{n} \in \mathsf{T}$, its label $(\mathfrak{x}, \mathfrak{w})$ is in $\mathcal{R}_{app}$.
2. For each $\mathsf{n} \in \mathsf{T}$, let $(\mathfrak{x}, \mathfrak{w})$ be its label. Let $\mathfrak{x} = (\mathsf{f}, \mathsf{args}, \mathsf{c}, \mathsf{f}_1, \mathsf{args}_1, \mathsf{f}_2, \mathsf{args}_2, \mathcal{O})$. Then

- $\mathsf{f} \in \mathrm{F}$.
- The number of its children is c.
- For $i \in [\mathsf{c}]$, let $(\mathsf{f}^i, \mathsf{args}^i, \mathsf{c}^i, \mathsf{f}^i_1, \mathsf{args}^i_1, \mathsf{f}^i_2, \mathsf{args}^i_2, \mathcal{O}^i)$ denote the first component of n's i'th child's label. Then $\mathsf{f}_i = \mathsf{f}^i$ and $\mathsf{args}_i = \mathsf{args}^i$.
- Let $\mathcal{O}$ be the multi-set union of $\mathfrak{x}.\mathcal{O}$ over all nodes' labels $(\mathfrak{x}, \mathfrak{w})$. Then $\mathcal{O}$ has output V.

Given a set of group elements F say it has *Merkle root* $\mathbf{r}$ if $\mathbf{r}$ is the root of a Merkle tree with the elements of F at the leaves using some pre-determined encoding.

We define a relation $\mathcal{R}_{\text{exec}}$ capturing knowledge of an execution of bounded length with a certain output set of records. $\mathcal{R}_{\text{exec}}$ consists of the pairs $(\mathrm{x}_{\text{exec}}, \mathrm{w}_{\text{exec}})$ of the form

- $\mathrm{x}_{\text{exec}} = (\mathbf{r}, C, \mathsf{V})$,
- $\mathrm{w}_{\text{exec}} = (n, \mathsf{T})$,

such that $n \leq C$, and T is a valid execution tree of length n with function set F having Merkle root $\mathbf{r}$, and output set V.

4 Repeated Computation with Global state

An RCG relation is defined by a pair of functions $(F, \mathscr{f})$.
We call $F(Z, W, Z^*, S) \to \{\mathsf{accept}, \mathsf{reject}\}$ the *transition predicate*.

We informally think of

- Z as the public input and W as the private input of F.
- Z^* as the output of F (although the actual output is $\{\mathsf{accept}, \mathsf{reject}\}$).
- S as the part of the private input that will be used in the final predicate.

Let D_1, D_2 be the domains of S, V respectively. $\mathscr{f}$ is a function $\mathscr{f} : D_1^* \times D_2 \to \{\mathsf{accept}, \mathsf{reject}\}$ called the *final predicate*.

The relation $\mathcal{R} = \mathcal{R}_{F,\mathscr{f}}$ consists of pairs (x, w) such that $x = (z_{final}, C, \mathsf{V}), w = (n, z = (z_0, \ldots, z_n), w = (w_1 \ldots, w_n), s = (s_1, \ldots, s_n))$ such that

- $z_0.\mathsf{init} = \mathsf{true}$.
- $z_n = z_{final}$.
- $n \leq C$.
- For each $i \in [n]$, $F(z_{i-1}, w_i, z_i, s_i) = \mathsf{accept}$.
- $\mathscr{f}(z_n, s_1, \ldots, s_n, \mathsf{V}) = \mathsf{accept}$.

We say a zk-SNARK for $\mathcal{R}$ is *space-efficient* if given s and streaming access to z and w $\mathbf{P}$ requires space $O(|F| + |s| + \log n)$.

4.1 Valid executions as RCGs

We show how to represent checking valid executions as defined in Section 3.3 via RCGs.

Define the function $F(Z, W, Z^*, S) \to \{\mathsf{accept}, \mathsf{reject}\}$ as follows.

- $Z = (g, \mathbf{r}, \mathsf{init})$ where g is a stack of elements of the form $(\mathsf{f}, \mathsf{args})$, $\mathbf{r}$ is a root of a Merkle tree, and init a boolean.
- $Z^* = (g^*, \mathbf{r}^*, \mathsf{init}^*)$ has the same form.
- $W = (\mathbf{p}, \mathbf{x}, \mathfrak{w})$
- S is a set of record operations.

Under this notation $F(Z, W, Z^*, S) = \mathsf{accept}$ if and only if

1. If $\mathsf{init} = \mathsf{true}$, g contains exactly one element.
2. Denoting $g[0] = (\mathsf{f}, \mathsf{args})$, we have $\mathsf{f} = \mathbf{x}.\mathsf{f}$ and $\mathsf{args} = \mathbf{x}.\mathsf{args}$.
3. Setting $\mathfrak{x} = (\mathbf{x}, S)$, we have $(\mathfrak{x}, \mathfrak{w}) \in \mathcal{R}_{app}$.
4. $\mathbf{p}$ is a Merkle path from f to $\mathbf{r}$.
5. $\mathbf{r} = \mathbf{r}^*$.
6. g^* is the result of popping $(\mathsf{f}, \mathsf{args})$ from g and then pushing the $\mathfrak{x}.\mathsf{c}$ elements $(\mathfrak{x}.\mathsf{f}_i, \mathsf{args}_i)$ for $i \in [\mathfrak{x}.\mathsf{c}]$.

Denote by g_{empty} the empty stack. We define the function $\mathscr{f}$ on input $(z_n, s_1, \ldots, s_n, \mathsf{V})$ to output accept if and only if $z_n.g = g_{empty}$, each s_i is a well-formed set of record operations, and when defining $\mathcal{O}$ as the multi-set union of $s_1, \ldots, s_n$ it has output V.

Lemma 4.1. *There is an efficiently computable and efficiently invertible map φ such that the following holds. Let* F *be a set of function commitments with Merkle root* $\mathbf{r}$*. Fix positive integers n, C with $n \leq C$. Define $z_{final} = (g_{empty}, \mathbf{r}, \mathsf{false})$. Let* T *be an execution tree of length n.*

Then $((\mathbf{r}, C, \mathsf{V}), \mathsf{T}) \in \mathcal{R}_{\text{exec}}$ if and only if $((z_{final}, C, \mathsf{V}), \varphi(\mathsf{T})) \in \mathcal{R}_{F,\mathscr{f}}$.

Proof. We describe the operation of φ. Given T of length n let $(\mathfrak{x}_1, \mathfrak{w}_1), \ldots, (\mathfrak{x}_n, \mathfrak{w}_n)$ be the labels of its nodes according to DFS order. Define a sequence of stacks $g_0, \ldots, g_n$ according to the sequence of labels.

Namely, g_0 is the stack containing only $(\mathfrak{x}_1.\mathsf{f}, \mathfrak{x}_1.\mathsf{args})$. And for each $i \in [n]$, g_i is the stack obtained by popping $g[0]$ and adding $(\mathfrak{x}_i.\mathsf{f}_j, \mathfrak{x}_i.\mathsf{args}_j)$ for $j \in [\mathfrak{x}_i.\mathsf{c}]$.

Now, define $z_0 = (g_0, \mathbf{r}, \mathsf{true})$ and for each $i \in [n]$, $z_i = (g_i, \mathbf{r}, \mathsf{false})$.

We now need to refer to the record operations in each instance separately. For this purpose, for each $i \in [n]$, denote $\mathfrak{x}_i = (\mathbf{x}_i, \mathcal{O}_i)$. For each $i \in [n]$, let $\mathbf{p}_i$ be the path from $\mathfrak{x}_i.\mathsf{f}$ to $\mathbf{r}$. Define for each $i \in [n]$, $w_i = (\mathbf{p}_i, \mathbf{x}_i, \mathfrak{w}_i)$, $s_i = \mathcal{O}_i$. Finally set $z = (z_0, \ldots, z_n), w = (w_1, \ldots, w_n), s = (s_1, \ldots, s_n)$ and $\varphi(\mathsf{T}) = (n, z, w, s)$. Given this definition of φ the statement of the lemma is straightforward to check. □

5 Removing the global state

Rational Identities: Following work on "log-derivative lookup" [Eag22, **?**], we characterize the validity of record operations via rational identites.

Claim 5.1. *Assume $\mathbb{F}$ has characteristic larger than $n+1$. Let V be a set of records and $\mathcal{O} = \{(op_i, v_i, vc_i, c_i)\}_{i\in[n]}$ be a set of record operations (defining $vc_i = 0$ when $op_i = \mathsf{add}$). Then $\mathcal{O}$ has output V if and only if the following rational function identities hold:*

1. $$\sum_{(v,c)\in\mathsf{V}} \frac{1}{X+vY+c} = \sum_{i\in[n],op_i=\mathsf{add}} \frac{1}{X+v_iY+c_i} - \sum_{i\in[n],op_i=\mathsf{del}} \frac{1}{X+v_iY+vc_i}.$$

2. *For some $m \in \mathbb{F}^n$, we have*
$$\sum_{i\in[n],op_i=\mathsf{add}} \frac{m_i}{X+v_iY+c_i} = \sum_{i\in[n],op_i=\mathsf{read}} \frac{1}{X+v_iY+vc_i}.$$

3. $$\sum_{i\in[n]} \frac{1}{X+c_i} = \sum_{i\in[n]} \frac{1}{X+i}.$$

Proof. We focus on the only if direction. That is, if $\mathcal{O}$ doesn't have output V one of the three identities should not hold. Let $M_{v,c} := \frac{1}{X+vY+c}$. The main fact we use is that the rational functions $\{M_{v,c}\}_{(v,c)\in\mathbb{F}^2}$ are linearly independent. Thus, $\sum_{v,c} a_{v,c}M_{v,c} = \sum b_{v,c}M_{v,c}$ implies $a_{v,c} = b_{v,c}$ for each $(v,c) \in \mathbb{F}^2$. The event of $\mathcal{O}$ not having output V means one of the following occurs.

1. The multi-set of counters $\{c_i\}_{i\in[n]}$ doesn't equal $\{1,\ldots,n\}$. In this case, the LHS of the third identity will not have all one coefficients for the elements $\{M_{0,c}\}_{i\in[n]}$ and so cannot equal the RHS.

   Note that when we are not in this case the counter in $\mathcal{O}$ are all distinct, which we assume for the next cases.

2. For some v, vc, c, $(\mathsf{del}, v, vc, c) \in \mathcal{O}$ but $(\mathsf{add}, v, vc) \notin \mathcal{O}$; or for some $v, vc, c_1 \neq c_2$, $(\mathsf{del}, v, vc, c_1), (\mathsf{del}, v, vc, c_2) \in \mathcal{O}$: In the first identity RHS, we will have $M_{v,vc}$ with coefficient in the range $\{-1,\ldots,-n\}$, while in the LHS it has coefficient one or zero.

3. V is *not* equal to the set V' of (v,c) for which $(\mathsf{add}, v, c) \in \mathcal{O}$ but $(\mathsf{del}, v, c) \notin \mathcal{O}$. We look at the first identity. V' is precisely the set of (v,c) with coefficient one on the RHS, while V is the set of (v,c) with coefficient one on the LHS. Hence the second identity cannot hold in this case.

4. For some v, vc, c, $(\mathsf{read}, v, vc, c) \in \mathcal{O}$ but $(\mathsf{add}, v, vc) \notin \mathcal{O}$: In the second identity RHS $M_{v,c}$ will have a coefficient in the range $\{1, \ldots, n\}$ while in the LHS it has coefficient zero.

□

We reduce the relation $\mathcal{R}_{F,\mathscr{f}}$ from the last section to $\mathcal{R}_{F^*,\mathscr{f}^*}$:
Let F denote the function $F(Z, W, Z^*, S) \to \{\mathsf{accept}, \mathsf{reject}\}$ as from Section 4.1.
Define the function $F^* : (Z, W, Z^*) \to \{\mathsf{accept}, \mathsf{reject}\}$:

- $Z = (Z_F, \hbar, \mathscr{s}, \alpha, \beta, \varepsilon)$.
- $Z^* = (Z_F^*, \hbar^*, \mathscr{s}^*, \alpha^*, \beta^*, \varepsilon^*)$.
- $W = (W_F, S_F, M)$

Under this notation $F^*(Z, W, Z^*) = \mathsf{accept}$ if and only if

1. $F(Z_F, W_F, Z_F^*, S_F) = \mathsf{accept}$.
2. Let $S_F = \{(op_i, v_i, vc_i, c_i)\}_{i\in[m]}$. We have
   $\mathscr{s}^* = \mathscr{s} +$
   $$\sum_{i\in[m];op_i=\mathsf{add}} \frac{1+\varepsilon m_i}{\alpha+\beta v_i+\ c_i} - \sum_{i\in[m];op_i=\mathsf{read}} \frac{\varepsilon}{\alpha+\beta v_i+vc_i} - \sum_{i\in[m];op_i=\mathsf{del}} \frac{1}{\alpha+\beta v_i+vc_i} + \sum_{i\in[m]} \frac{\varepsilon^2}{\alpha+c_i}.$$
3. $\alpha^* = \alpha, \beta^* = \beta, \varepsilon^* = \varepsilon$.
4. $\hbar^* = \mathcal{H}(\hbar, \mathsf{cm}(S_F, M))$.

$\mathscr{f}^*(Z, \mathsf{V}) = \mathsf{accept}$ if and only if

1. $\mathscr{s} = \sum_{(v,c)\in\mathsf{V}} \frac{1}{\alpha+\beta v+c} + \sum_{i\in[n]} \frac{\varepsilon^2}{\alpha+i}$,
2. $\mathcal{H}(\hbar, \mathsf{V}, 1) = \alpha$, $\mathcal{H}(\hbar, \mathsf{V}, 2) = \beta$, $\mathcal{H}(\hbar, \mathsf{V}, 3) = \varepsilon$.

Lemma 5.2. *There is an efficiently computable and efficiently invertible map φ such that the following holds. Let* F *be a set of function commitments with Merkle root* $\mathbf{r}$*. Fix positive integers n, C with $n \le C$. Fix some $\alpha, \beta, \varepsilon \in \mathbb{F}$ and set of records* V*. Define $z_{final} = (g_{empty}, \mathbf{r}, \mathsf{false}), z^*_{final} := (z_{final}, \hbar, \mathscr{s}, \alpha, \beta, \varepsilon)$ and set $\phi := (z^*_{final}, C, \mathsf{V})$. Assume the ZTA for the appropriate family of functions appearing in the proof. Suppose efficient $\mathcal{A}$ outputs ω such that $(\phi, \omega) \in \mathcal{R}_{F^*,\mathscr{f}^*}$.*

Let $\mathcal{D}$ be the appropriate family of functions to be defined in the proof. Assume that cm *is collision resistant and the ZTA holds for $(\mathcal{D}, \mathcal{H}, \mathsf{cm}, n)$. Then e.w.p.* $\mathsf{negl}(\lambda)$*, $((z_{final}, C, \mathsf{V}), \varphi(\omega)) \in \mathcal{R}_{F,\mathscr{f}}$.*

Proof. Given a witness $\omega = (n, z', w')$ with $z' = (z'_0, \ldots, z'_n), w' = (w'_1, \ldots, w'_n)$ output by $\mathcal{A}$, denote $z'_i = (z_i, \hbar_i, \mathit{s}_i, \alpha_i, \beta_i, \varepsilon_i), w'_i = (w_i, s_i, M_i)$. Define $\omega = \varphi(\omega)$ as $\omega := (n, (z_0, \ldots, z_n), (w_1, \ldots, w_n), (s_1, \ldots, s_n))$. From $(\phi, \omega) \in \mathcal{R}_{F^*, \mathscr{f}^*}$, we know ω satisfies the transition constraints, namely for $i \in [n]$, $F(z_{i-1}, w_i, z_i, s_i) = \mathsf{accept}$. We also know that $z_0.\mathsf{init} = \mathsf{true}$, $z_n = z_{\mathit{final}}$, and $n \leq C$. It is left to show that e.w.p. $\mathsf{negl}(\lambda)$ $\mathscr{f}(z_n, s_1, \ldots, s_n, \mathsf{V}) = \mathsf{accept}$.

From $((z^*_{\mathit{final}}, C, \mathsf{V}), \omega) \in \mathcal{R}_{F^*, \mathscr{f}^*}$ we know the equations from Claim 5.1 hold at $\alpha, \beta, \varepsilon$. That is, defining the rational function

$$
\begin{aligned}
r(X, Y, Z) := & \sum_{(v,c) \in \mathsf{V}} \frac{1}{X + vY + c} - \sum_{i \in [n], \mathit{op}_i = \mathsf{add}} \frac{1}{X + v_i Y + c_i} + \sum_{i \in [n], \mathit{op}_i = \mathsf{del}} \frac{1}{X + v_i Y + v c_i} \\
& + Z \left(\sum_{i \in [n], \mathit{op}_i = \mathsf{add}} \frac{m_i}{X + v_i Y + c_i} - \sum_{i \in [n], \mathit{op}_i = \mathsf{read}} \frac{1}{X + v_i Y + v c_i} \right) \\
& + Z^2 \left(\sum_{i \in [n]} \frac{1}{X + c_i} - \sum_{i \in [n]} \frac{1}{X + i} \right),
\end{aligned}
$$

we have $r(\alpha, \beta, \varepsilon) = 0$. If any of the three rational identities from Claim 5.1 does not hold, we have $r(X, Y, Z) \not\equiv 0$. Let $f \in \mathbb{F}_{\leq d}[X, Y, Z]$ denote the resulting non-zero polynomial when multiplying $r(X, Y, Z)$ with all of its denominators. Note that $f(\alpha, \beta, \varepsilon) = 0$. Define D as the function that computes $f(X, Y, Z)$ given $x := \omega$, $\tau := \mathsf{V}$, and set $\mathcal{D} := \{D\}$. Then we can define an efficient adversary $\mathcal{A}'$ against the 3-variate ZTA for $(\mathcal{D}, \mathcal{H}, \mathsf{cm}, d)$ that outputs the degree-d relation (D, x, τ), which has probability $\mathsf{negl}(\lambda)$. □

Definition 5.3 (t-variate ZTA)**.** *Fix $\mathsf{cm} : \mathbb{F}^M \to K$, hash function $\mathcal{H}$, and integer d. Fix the family of functions $\mathcal{D}$. We say the tuple (D, x, τ) is a* degree-d relation for $(\mathcal{D}, \mathcal{H}, \mathsf{cm})$ *if*

1. $D \in \mathcal{D}$.
2. $f(X_1, \ldots, X_t) := D(x, \tau)$ *is a non-zero element of* $\mathbb{F}_{\leq d}[X_1, \ldots, X_t]$.
3. *Setting* $z_i := \mathcal{H}(\mathsf{cm}(x), \tau, i)$ *for* $i \in [t]$, *we have* $f(z_1, \ldots, z_t) = 0$.

The t-variate Zero-Testing Assumption (ZTA) for $(\mathcal{D}, \mathcal{H}, \mathsf{cm}, d)$ states that for any efficient $\mathcal{A}$, the probability that $\mathcal{A}$ outputs a degree-d relation for $(\mathcal{D}, \mathcal{H}, \mathsf{cm})$ is $\mathsf{negl}(\lambda)$.

Lemma 5.4. *Fix a family of functions $\mathcal{D}$ whose outputs are polynomials in $\mathbb{F}_{\leq d}[X_1, \ldots, X_t]$. Let $\mathcal{D}_t$ be a family of functions to be defined in the proof. Then the univariate ZTA for $(\mathcal{D}_t, \mathcal{H}, \mathsf{cm}, d)$ implies the t-variate ZTA for $(\mathcal{D}, \mathcal{H}, \mathsf{cm}, d)$ and $t = \mathsf{poly}(\lambda)$.*

Proof. Let $\mathcal{A}$ be an adversary against the t-variate ZTA that outputs the degree-d relation (D, x, τ) for $(\mathcal{D}, \mathcal{H}, \mathsf{cm})$. We construct the adversary $\mathcal{A}'$ against the univariate ZTA

that outputs a degree-d relation for $(\mathcal{D}_t, \mathcal{H}, \mathsf{cm})$, where $\mathcal{D}_t$ will be the union of all the functions D_i defined in the following.

Write $f(X_1, \ldots, X_t) := D(x, \tau)$ as a polynomial in X_t over $\mathbb{F}[X_1, \ldots, X_{t-1}]$:

$$f(X_t) = \sum_{i=0}^{d} C_i(X_1, \ldots, X_{t-1}) X_t^i.$$

Suppose first that $f(z_1, \ldots, z_{t-1}, X_t) \not\equiv 0$. Then $\mathcal{A}'$ can output the degree-d relation (D_t, x, τ_t), where D_t is the function that computes $f_t(X) := f(z_1, \ldots, z_{t-1}, X)$ given x and $\tau_t := (\tau, t)$. Note that $f_t(z_t) = 0$ with $z_t = \mathcal{H}(\mathsf{cm}(x), \tau_t)$.

Otherwise, there is a non-zero polynomial $C_i \in \mathbb{F}_{\leq d}[X_1, \ldots, X_{t-1}]$ which satisfies $C_i(z_1, \ldots, z_{t-1}) = 0$. If $C_i(z_1, \ldots, z_{t-2}, X_{t-1}) \not\equiv 0$, $\mathcal{A}'$ can output the degree-d relation (D_{t-1}, x, τ_{t-1}), where D_{t-1} is the function that computes $f_{t-1}(X) := C_i(z_1, \ldots, z_{t-2}, X)$ given x and $\tau_{t-1} := (\tau, t-1)$.

Recursively define degree-d relations (D_i, x, τ_i) until $i = 1$ and we have a univariate non-zero polynomial $C_i \in \mathbb{F}_{\leq d}[X_1]$ with $C_i(z_1) = 0$. In this base case, $\mathcal{A}'$ can output the degree-d relation (D_1, x, τ_1), where D_1 is the function that computes $f_1(X) := C_i(X)$ given x and $\tau_1 := (\tau, 1)$, finishing the proof. □

6 Non-interactive folding schemes

We fix a vector space K over $\mathbb{F}$, and an $\mathbb{F}$-linear function $\mathsf{cm} : \mathbb{F}^M \to K$ that will be an implicit parameter in Definition 6.1. We say a relation $\mathcal{R}$ is cm-*compatible* if every element of $\mathcal{R}$ has the form $(\mathsf{cm}(\omega), \omega)$. We say $\mathcal{R}$ is cm-*extendable* if every element of $\mathcal{R}$ has the form $((\mathsf{cm}(\omega), \tau), \omega)$ for some ω, τ.

Definition 6.1. *Fix relations $\mathcal{R}$ and $\mathcal{R}_{\mathfrak{acc}}$ that are respectively* cm*-compatible and* cm*-extendable. An $(\mathcal{R} \mapsto \mathcal{R}_{\mathfrak{acc}})$-*folding scheme *is a pair of algorithms $(\mathbf{P}, \mathbf{V})$ such that*

1. $\mathbf{P}$ *on input $(\Phi, \phi'; \omega, \omega')$ produces a pair (Φ^*, ω^*) and proof π.*
2. $\mathbf{V}$ *on input $(\Phi, \phi', \Phi^*, \pi)$ outputs* accept *or* reject *such that*
   (a) ***Completeness:*** *If $(\Phi, \omega) \in \mathcal{R}_{\mathfrak{acc}}$, $(\phi', \omega') \in \mathcal{R}$, and $\mathbf{P}(\Phi, \phi'; \omega, \omega') = (\pi, \Phi^*, \omega^*)$ then with probability $1 - \mathsf{negl}(\lambda)$, $(\Phi^*, \omega^*) \in \mathcal{R}_{\mathfrak{acc}}$ and $\mathbf{V}(\Phi, \phi', \Phi^*, \pi) =$* accept.
   (b) ***Knowledge soundness given extractable commitments:***
   For any efficient $\mathcal{A}$ the probability of the following event is $\mathsf{negl}(\lambda)$: $\mathcal{A}$ outputs $(\phi, \tau), \phi', (\phi^*, \tau^*), \omega, \omega', \omega^*, \pi$ such that
      i. $\mathsf{cm}(\omega) = \phi, \mathsf{cm}(\omega') = \phi', \mathsf{cm}(\omega^*) = \phi^*$,
      ii. $\mathbf{V}(\phi, \phi', \phi^*, \pi) =$ accept,
      iii. $((\phi^*, \tau^*), \omega^*) \in \mathcal{R}_{\mathfrak{acc}}$,
      iv. $((\phi, \tau), \omega) \notin \mathcal{R}_{\mathfrak{acc}}$ *or* $(\phi', \omega') \notin \mathcal{R}$.

Remark 6.2. *The justification for requiring only knowledge soundness given extractable commitments is as follows. We assume the Algebraic Group Model [FKL18] and use a commitment scheme based on linear combination of group elements like [KZG10]. In this model with such a commitment scheme an adversary $\mathcal{A}$ must output ω, with $\mathsf{cm}(\omega) = \phi$ whenever it outputs some $\phi \in K$. For more details see [FKL18] or Section 2.2 of [GWC19], as well as Section 7 of this paper.*

6.1 Relations for folding schemes

We define a more general satisfiability relation than in [**?**]. We have as parameters, integers $n, \mathscr{M}, d$ and an $\mathbb{F}$-vector space K. We have a

- *Constraint function* $f : \mathbb{F}^{\mathscr{M}} \to \mathbb{F}^n$ which is a vector of n $\mathscr{M}$variate polynomials of degree $\leq d$,
- *Instance predicate* $\mathsf{f} : K \to \{\mathsf{accept}, \mathsf{reject}\}$,
- *Commitment function* $\mathsf{cm} : \mathbb{F}^{\mathscr{M}} \to K$ which is $\mathbb{F}$-linear and assumed to be collision resistant.

Given $(f, \mathsf{f}, \mathsf{cm})$ we define a relation $\mathcal{R}_{f,\mathsf{f},\mathsf{cm}}$ consisting of all pairs (ϕ, ω) such that

1. $f(\omega) = 0^n$.
2. $\mathsf{f}(\phi) = \mathsf{accept}$.
3. $\phi = \mathsf{cm}(\omega)$.

The relation $\mathcal{R}^{\mathsf{rand}}$: For brevity, let $\mathcal{R} = \mathcal{R}_{f,\mathsf{f},\mathsf{cm}}$. As in [**?**], we define the "randomized relaxed" version of $\mathcal{R}, \mathcal{R}^{\mathsf{rand}}$. First, some required notation. Let $t := \log n$. For $i \in [n]$, let $S \subset \{0, \ldots, t-1\}$ be the set such that $i - 1 = \sum_{j \in [S]} 2^j$. We define the t-variate polynomial pow_i as

$$\mathsf{pow}_i(X_0, \ldots, X_{t-1}) := \prod_{\ell \in S} X_\ell.$$

Note that if $\boldsymbol{\beta} = (\beta, \beta^2, \beta^4, \ldots, \beta^{2^{t-1}})$, $\mathsf{pow}_i(\boldsymbol{\beta}) = \beta^{i-1}$.

Given the above notation, $\mathcal{R}^{\mathsf{rand}}$ consists of the pairs (Φ, ω) with $\Phi = (\phi, \boldsymbol{\beta}, e)$ such that

1. $\phi = \mathsf{cm}(\omega)$.
2. $\boldsymbol{\beta} \in \mathbb{F}^t, e \in \mathbb{F}$ and we have

$$\sum_{i \in [n]} \mathsf{pow}_i(\boldsymbol{\beta}) f_i(\omega) = e.$$

(Here, f_i denotes the i'th output coordinate of f.)

6.2 The PROTO**galaxy** scheme

Deviating from [**?**], we explicitly present PROTO**GALAXY** as a *non-interactive* folding scheme, and for the special case of folding $k = 1$ instances. We define $Z(X) := X \cdot (1-X)$. We assume below $\mathcal{H}$ is a function mapping arbitrary strings to elements of $\mathbb{F}^*$.

$\underline{\mathbf{P}_{PG}(\Phi = (\phi, \boldsymbol{\beta}, e), \phi_1; \omega, \omega_1)}$:

1. Compute $\delta = \mathcal{H}(\Phi, \phi_1)$. Define $\boldsymbol{\delta} := (\delta, \delta^2, \ldots, \delta^{2^{t-1}}) \in \mathbb{F}^t$.
2. Compute the polynomial
$$F(X) := \sum_{i \in [n]} \mathsf{pow}_i(\boldsymbol{\beta} + X\boldsymbol{\delta}) f_i(\omega).$$
(Note that $F(0) = \sum_{i \in [n]} \mathsf{pow}_i(\boldsymbol{\beta}) f_i(\omega) = e$.)
3. Denote the non-constant coefficients of F by $a := (F_1, \ldots, F_t)$.
4. Compute $\alpha = \mathcal{H}(\Phi, \phi_1, a)$.
5. Compute $\boldsymbol{\beta}^* \in \mathbb{F}^t$ where $\boldsymbol{\beta}^*_i := \boldsymbol{\beta}_i + \alpha \cdot \boldsymbol{\delta}_i$.
6. Define the polynomial $G(X)$ as
$$G(X) := \sum_{i \in [n]} \mathsf{pow}_i(\boldsymbol{\beta}^*) f_i(X \cdot \omega + (1 - X)\omega_1).$$
7. Compute the polynomial $K(X)$ such that
$$G(X) = F(\alpha)X + Z(X)K(X).$$
8. Let $b := (K_0, \ldots, K_{d-2})$ be the coefficients of $K(X)$.
9. Compute $\gamma = \mathcal{H}(\Phi, \phi_1, a, b)$.
10. Compute
$$e^* := F(\alpha)\gamma + Z(\gamma)K(\gamma).$$

Finally, output

- the instance $\Phi^* = (\phi^*, \boldsymbol{\beta}^*, e^*)$, where
$$\phi^* := \gamma \cdot \phi + (1 - \gamma)\phi_1,$$
- the witness $\omega^* := \gamma \cdot \omega + (1 - \gamma) \cdot \omega_1$,
- and the proof $\pi := (a, b)$.

$\underline{\mathbf{V}_{PG}(\Phi, \phi_1, \Phi^*, \pi = (a, b)) :}$

1. Check that $\mathsf{f}(\phi_1) = \mathsf{accept}$. Output reject otherwise.
2. Compute $\delta, \alpha, \boldsymbol{\beta}^*, \gamma$ as in the prover algorithm given Φ, ϕ_1, a, b.
3. Check that Φ^* is computed as in the prover algorithm. Output accept iff this is the case.

For the knowledge soundness analysis we'll use a variant of the Zero-Testing assumption from [LS24].

Definition 6.3. *Fix $\mathsf{cm} : \mathbb{F}^M \to K$, hash function $\mathcal{H}$, and integer d. Fix the family of functions $\mathcal{D}$. We say the tuple (D, x, τ) is a* degree d-relation for $(\mathcal{D}, \mathcal{H}, \mathsf{cm})$ *if*

1. *$D \in \mathcal{D}$.*
2. *$f(X) := D(x, \tau)$ is a non-zero element of $\mathbb{F}_{\leq d}[X]$.*
3. *Setting $z := \mathcal{H}(\mathsf{cm}(x), \tau)$, we have $f(z) = 0$.*

The Zero-Testing Assumption (ZTA) for $(\mathcal{D}, \mathcal{H}, \mathsf{cm}, d)$ states that for any efficient $\mathcal{A}$, the probability that $\mathcal{A}$ outputs a degree d-relation for $(\mathcal{D}, \mathcal{H}, \mathsf{cm})$ is $\mathsf{negl}(\lambda)$.

Theorem 6.4. *Set $d' := \max\{n, d\}$. Denote $\mathsf{cm}'((\omega, \boldsymbol{\beta}, e), \omega_1) := ((\mathsf{cm}(\omega), \boldsymbol{\beta}, e), \mathsf{cm}(\omega_1))$. Let $\mathcal{D}$ be a family of four functions to be defined in the proof. Assume that cm is collision resistant and the ZTA holds for $(\mathcal{D}, \mathcal{H}, \mathsf{cm}', d')$. Then* ProtoGalaxy *is a $(\mathcal{R} \mapsto \mathcal{R}^{\mathsf{rand}})$-folding scheme.*

Proof. The main thing to prove is knowledge soundness given extractable commitments. Fix any efficient $\mathcal{A}$. Let E be the event that $\mathcal{A}$ outputs $\Phi = (\phi, \boldsymbol{\beta}, e), \phi_1, \Phi^* = (\phi^*, \boldsymbol{\beta}^*, e^*)$, $\omega, \omega_1, \omega^*, \pi$ such that

1. $\mathsf{cm}(\omega) = \phi, \mathsf{cm}(\omega_1) = \phi_1, \mathsf{cm}(\omega^*) = \phi^*$,
2. $\mathbf{V}_{PG}(\Phi, \phi_1, \Phi^*, \pi) = \mathsf{accept}$,
3. $(\Phi^*, \omega^*) \in \mathcal{R}^{\mathsf{rand}}$,
4. $(\Phi, \omega) \notin \mathcal{R}^{\mathsf{rand}}$ or $(\phi_1, \omega_1) \notin \mathcal{R}$.

According to Definition 6.1, knowledge soundness is equivalent to E having probability $\mathsf{negl}(\lambda)$ for any such $\mathcal{A}$. We construct an efficient $\mathcal{A}'$ that runs $\mathcal{A}$, and when E occurs outputs either a collision of cm or a degree d'-relation for $(\mathcal{H}, \mathsf{cm})$. By the theorem assumption this implies E is contained in two events of probability $\mathsf{negl}(\lambda)$, and must have probability $\mathsf{negl}(\lambda)$ itself.

Assume we are in event E. Using linearity of cm, when E occurs we have

$$\mathsf{cm}(\gamma\omega + (1-\gamma)\omega_1) = \gamma\phi + (1-\gamma)\phi_1 = \phi^* = \mathsf{cm}(\omega^*).$$

Thus, if $\omega^* \neq \gamma\omega + (1-\gamma)\omega_1$, $\mathcal{A}'$ can output $(\omega^*, \gamma\omega + (1-\gamma)\omega_1)$ as a collision of cm. Now assume that $\omega^* = \gamma\omega + (1-\gamma)\omega_1$. Suppose $\pi = (a, b)$, with $a = (a_1, \ldots, a_t), b = (b_0, \ldots, b_{d-2})$. Define $F_0(X) := e + \sum_{i\in[t]} a_i X^i, K'(X) := \sum_{i=0}^{d-2} b_i X^i$. Let $\delta, \boldsymbol{\delta}, \alpha, \boldsymbol{\beta}^*, \gamma$ be computed as in the prover description given a, b. Define the polynomials

$$F'(X) := F_0(X) - \sum_{i\in[n]} \mathsf{pow}_i(\boldsymbol{\beta} + X\boldsymbol{\delta}) f_i(\omega),$$
$$G'(X) := F_0(\alpha)X + Z(X)K'(X) - \sum_{i\in[n]} \mathsf{pow}_i(\boldsymbol{\beta}^*) f_i(X\omega + (1-X)\omega_1).$$

Since $((\phi^*, \boldsymbol{\beta}^*, e^*), \omega^*) \in \mathcal{R}^{\mathsf{rand}}$ and $\mathbf{V}_{PG}(\Phi, \phi', \Phi^*, \pi) = \mathsf{accept}$,

$$\begin{aligned} G'(\gamma) &= F_0(\alpha)\gamma + Z(\gamma)K'(\gamma) - \sum_{i\in[n]} \mathsf{pow}_i(\boldsymbol{\beta}^*) f_i(\gamma\omega + (1-\gamma)\omega_1) \\ &= e^* - \sum_{i\in[n]} \mathsf{pow}_i(\boldsymbol{\beta}^*) f_i(\omega^*) = e^* - e^* = 0. \end{aligned}$$

Set $x := ((\omega, \boldsymbol{\beta}, e), \omega_1)$ and $\tau_1 := (a, b)$. If $G' \not\equiv 0$, $\mathcal{A}'$ outputs the degree d'-relation (D_1, x, τ_1), where D_1 is the function that computes $G'(X)$ given x, τ_1.

Assume now that $G' \equiv 0$.

If $(\phi_1, \omega_1) \notin \mathcal{R}$, using $Z(0) = 0$ we have

$$G'(0) = -\sum_{i\in[n]} \mathsf{pow}_i(\boldsymbol{\beta}^*) f_i(\omega_1) = 0.$$

Define the polynomial $A(X) := \sum_{i\in[n]} f_i(\omega_1)\mathsf{pow}_i(\boldsymbol{\beta}_1 + X\delta, \boldsymbol{\beta}_2 + X\delta^2, \ldots, \boldsymbol{\beta}_t + X\delta^{2^{t-1}})$. We have $A(\alpha) = 0$. Suppose first that $A(X) \not\equiv 0$. Then setting D_2 to be the function that computes $A(X)$ given x and $\tau_2 := a$, $\mathcal{A}'$ can output the degree n relation (D_2, x, τ_2). Now assume $A(X) \equiv 0$. Define the polynomial

$$B(X, Y) := \sum_{i\in[n]} f_i(\omega_1)\mathsf{pow}_i(\boldsymbol{\beta}_1 + XY, \boldsymbol{\beta}_2 + XY^2, \ldots, \boldsymbol{\beta}_t + XY^{2^{t-1}}).$$

We have that $B(X, \delta) \equiv 0$. Write $B(X, Y)$ as a polynomial in X over $\mathbb{F}[Y]$:

$$B(X) = \sum_{i=0}^{t} C_i(Y) X^i.$$

Because we're in the case $(\phi_1, \omega_1) \notin \mathcal{R}$, B is a combination of the n linearly independent polynomials $\left\{\mathsf{pow}_i(\boldsymbol{\beta}_1 + XY, \boldsymbol{\beta}_2 + XY^2, \ldots, \boldsymbol{\beta}_t + XY^{2^{t-1}})\right\}_{i\in[n]}$ with at least one non-zero coefficient, and so $B(X, Y) \not\equiv 0$. This means one of the polynomials C_i is non-zero, while $C_i(\delta) = 0$. We can use this to let $\mathcal{A}'$ output the degree n relation (D_3, x, τ_3), where D_3 is the function that computes C_i given x and $\tau_3 := \emptyset$.

Now, assume that $(\Phi, \omega) \notin \mathcal{R}^{\mathsf{rand}}$. As we're still assuming $G' \equiv 0$, we have

$$G'(1) = F_0(\alpha) - \sum_{i \in [n]} \mathsf{pow}_i(\boldsymbol{\beta}^*) f_i(\omega) = 0.$$

But we also have $F'(\alpha) = G'(1)$ and so $F'(\alpha) = 0$. On the other hand,

$$F'(0) = e - \sum_{i \in [n]} \mathsf{pow}_i(\boldsymbol{\beta}) f_i(\omega) \neq 0.$$

Setting $\tau_4 := a$ and D_4 to be the function that computes F' given x, τ_4, we have that (D_4, x, τ_4) is a degree $\log n$ relation that $\mathcal{A}'$ can output in this case. Setting $\mathcal{D} = \{D_1, D_2, D_3, D_4\}$ we have proven knowledge soundness under the theorem assumptions. □

7 Adversaries supporting recursive extraction

Following [LS24], we define a model of "recursive extraction" for our analysis in Section 8. We assume our commitment function $\mathsf{cm} : \mathbb{F}^{\mathscr{M}} \to K$ is surjective. We assume the existence of an efficiently computable injective representation function $R : K \to \mathbb{F}^{\ell}$. Whenever an adversary $\mathcal{A}$ outputs $a \in K$ we assume it is represented as $R(a)$. When analyzing knowledge soundness of our zk-SNARK in the next section, we put the following limitation on $\mathcal{A}$. Say $\mathcal{A}$ outputs a vector v over $\mathbb{F}$. If there is an index i such that $(v_i, \ldots, v_{i+\ell-1}) = R(a)$ for some $a \in K$, then $\mathcal{A}$ must also output $\omega \in \mathbb{F}^{\mathscr{M}}$ such that $\mathsf{cm}(\omega) = a$.

This assumption is motivated by a "recursive" interpretation of the Algebraic Group Model[FKL18] as done in [LS24]. For illustration, consider first the case where $\mathsf{cm} : \mathbb{F}^n \to \mathbb{G}$ is defined as $\mathsf{cm}(\omega) =< \omega, V >$ for a fixed vector $V \in \mathbb{G}^n$ derived in a setup procedure. I.e. cm is a Pedersen commitment in this case. In this case, the AGM forces $\mathcal{A}$ when outputting $a \in \mathbb{G}$ to also output ω such that $< \omega, V >= \mathsf{cm}(\omega) = a$. [LS24] now raise the idea that if a prespecified subset of indices of ω is a valid representation of $b \in \mathbb{G}$, it is reasonable to demand of an algebraic $\mathcal{A}$ to also output ω_2 with $< \omega_2, V >= b$.

Our concrete choice for cm when using ProtoGalaxy, is of the following form.[1] We have a setup procedure outputting a vector of group elements $V \in \mathbb{G}^n$ is output. We have some fixed partition of our input $\omega \in \mathbb{F}^{\mathscr{M}}$ into continuous segments of size either one or n. To get $\mathsf{cm}(\omega)$ we operate segment-wise. If the segment ω_i is of size one we simply append ω_i to the output. If a segment $s = (\omega_i, \ldots, \omega_{i+n-1})$ is of size n we append $< s, V >$ to the output. In particular the output $\mathsf{cm}(\omega)$ is a mixture of $\mathbb{F}$ and $\mathbb{G}$ elements, and accordingly the space K is a direct sum of spaces $\mathbb{V}_i \in \{\mathbb{F}, \mathbb{G}\}$. It follows that an algebraic adversary outputting $c \in K$ must output ω with $\mathsf{cm}(\omega) = c$ as the AGM forces it to send an opening $s \in \mathbb{F}^n$ to each $a \in \mathbb{G}$.

[1] cm is of this form because it is derived from an interactive protocol where the prover messages are in committed form, but verifier challenges are in the clear. See [BC23, **?**] for more details.

8 The main construction

We say a pair of functions $(F, \not{\ell})$ used to define an RCG relation $\mathcal{R}_{F,\not{\ell}}$ is *trivial* if the S variable is not used in F, and accordingly $\not{\ell}$ depends only on (z_{final}, V). We assume in this section $(F, \not{\ell})$ is trivial, thinking of it as equal to $(F^*, \not{\ell}^*)$ from Section 5.

8.1 The extended function F'

As in [KST21, BCL$^+$21], we first describe an extended function F' that executes the folding verifier in addition to an iteration of F. Loosely speaking, extending F into F' is what enables bootstrapping a folding scheme into an IVC or RCG. We describe the function arguments first.

$\mathfrak{x} = (z, \mathsf{count}, \hbar)$

- z - output for F
- count - counter of IVC step
- $\hbar$ - hash of accumulator

$\mathfrak{w} = (\Phi^*, \Phi, \mathfrak{x}_0, w, \pi)$

- Φ^* - current accumulator instance
- Φ - previous accumulator instance
- $\mathfrak{x}_0$ - instance (of F') to be accumulated.
- w - private input for F
- π - proof for ProtoGalaxy verifier

$F'(\mathfrak{x}, \mathfrak{w}) = \mathsf{accept}$ if and only if:

1. $F(\mathfrak{x}_0.z, w, z) = \mathsf{accept}$
2. If $\mathsf{count} > 1$:
   (a) $\mathcal{H}(\Phi^*) = \hbar$.
   (b) $\mathfrak{x}_0.\hbar = \mathcal{H}(\Phi)$.
   (c) $\mathfrak{x}_0.\mathsf{count} = \mathsf{count} - 1$.
   (d) $\mathbf{V}_{PG}(\Phi, \mathfrak{x}_0, \pi, \Phi^*) = \mathsf{accept}$.
3. If $\mathsf{count} = 1$:
   - $\mathfrak{x}_0.z.\mathsf{init} = \mathsf{true}$

Let $\mathcal{R}, \mathcal{R}^{\mathsf{rand}}$ be relations for the PROTOGALAXY version of the function F' above.[2]

For readability, from now on we modify notational conventions and denote an accumulator by acc, accumulator witness by $\mathbf{w}$-acc, instance by inst, and instance witness by $\boldsymbol{w}$-inst.

8.2 The relation $\mathcal{R}_{\mathsf{fin}}$

We define the relation $\mathcal{R}_{\mathsf{fin}}$ of pairs $(\boldsymbol{x}, \boldsymbol{w})$ such that

- $\boldsymbol{x} = (\mathsf{acc}, \mathsf{V}, C, z_{final})$
- $\boldsymbol{w} = (\mathbf{w}\text{-}\mathsf{acc}, \mathsf{acc}_0, \mathsf{inst}, \pi)$

such that

1. $(\mathsf{acc}, \mathbf{w}\text{-}\mathsf{acc}) \in \mathcal{R}^{\mathsf{rand}}$.
2. $\mathbf{V}_{PG}(\mathsf{acc}_0, \mathsf{inst}, \pi, \mathsf{acc}) = \mathsf{accept}$.
3. $\mathcal{H}(\mathsf{acc}_0) = \mathsf{inst}.\hbar$.
4. $\mathsf{inst}.z = z_{final}$.
5. $\mathsf{inst}.\mathsf{count} \leq C$.

Let $(\mathbf{P}_{\mathsf{fin}}, \mathbf{V}_{\mathsf{fin}})$ be a zk-SNARK for $\mathcal{R}_{\mathsf{fin}}$.

8.3 The final construction

We now describe the full prover and verifier for a given trivial RCG relation $\mathcal{R}_{F,\mathscr{f}}$ Later we review how to use this to get a zk-SNARK for the relation $\mathcal{R}_{\text{exec}}$ of valid executions, given the reductions of previous sections.

$\underline{\mathbf{P}(x, w)}$:

1. Let $\boldsymbol{x} = (z_{final}, C, \mathsf{V}), w = (n, (z_0, \ldots, z_n), (w_1, \ldots, w_n))$. Recall that $(\boldsymbol{x}, w) \in \mathcal{R}_{F,\mathscr{f}}$ implies $F(z_{i-1}, w_i, z_i) = \mathsf{accept}$ for each $i \in [n]$, $z_0.\mathsf{init} = \mathsf{true}, z_n = z_{final}$ and $\mathscr{f}(z_{final}, \mathsf{V}) = \mathsf{true}$.
2. Choose instance $\mathsf{inst}_0 = (z_0, \mathsf{count}_0, \hbar_0)$ for arbitrary values $\mathsf{count}_0, \hbar_0$. Choose acc_0 arbitrarily. Let $\mathsf{inst}_1 = (z_1, 1, \hbar_1)$, $\boldsymbol{w}$-$\mathsf{inst}_1 = (\mathsf{acc}_0, \mathsf{acc}_0, \mathsf{inst}_0, w_1, \pi_0)$ for arbitrary values $\hbar_1, \mathsf{acc}_0, \pi_0$. (We can choose some values arbitrarily as they aren't constrained in F' when $\mathsf{count} = 1$.)

[2] In an updated version of the paper we will give more details on how to efficiently implement F' as a PROTOGALAXY relation.

3. Let acc_1 be a randomly chosen satisfiable accumulator. Namley, $\mathsf{acc}_1 = (\mathsf{cm}(\mathbf{w}\text{-}\mathsf{acc}_1), \boldsymbol{\beta}, e)$ where $\mathbf{w}\text{-}\mathsf{acc}_1$ and $\boldsymbol{\beta}$ are chosen randomly[3], and e is set to $e = \sum_{i\in[n]} \mathsf{pow}_i(\boldsymbol{\beta}) f_i(\mathbf{w}\text{-}\mathsf{acc}_1)$.
4. For each $2 \leq i \leq n$, compute
   (a) $(\mathsf{acc}_i, \mathbf{w}\text{-}\mathsf{acc}_i, \pi_i) = \mathbf{P}^{\mathrm{PG}}_{\mathsf{cm},n,f}(\mathsf{acc}_{i-1}, \mathbf{w}\text{-}\mathsf{acc}_{i-1}, \mathsf{inst}_{i-1}, \boldsymbol{w}\text{-}\mathsf{inst}_{i-1})$
   (b) $\mathsf{inst}_i = (z_i, i, \mathcal{H}(\mathsf{acc}_i))$,
   (c) $\boldsymbol{w}\text{-}\mathsf{inst}_i = (\mathsf{acc}_i, \mathsf{acc}_{i-1}, \mathsf{inst}_{i-1}, w_i, \pi_i)$
5. $(\mathsf{acc}, \mathbf{w}\text{-}\mathsf{acc}, \pi^*) = \mathbf{P}^{\mathrm{PG}}_{\mathsf{cm},n,f}(\mathsf{acc}_n, \mathbf{w}\text{-}\mathsf{acc}_n, \mathsf{inst}_n, \boldsymbol{w}\text{-}\mathsf{inst}_n)$.
6. Let $\pi_{\mathsf{fin}} = \mathbf{P}_{\mathsf{fin}}(\boldsymbol{x}, \boldsymbol{w})$ where
   - $\boldsymbol{x} = (\mathsf{acc}, \mathsf{V}, C, z_{final})$
   - $\boldsymbol{w} = (\mathbf{w}\text{-}\mathsf{acc}, \mathsf{acc}_n, \mathsf{inst}_n, \pi^*)$
7. Output $\pi = (\mathsf{acc}, \pi_{\mathsf{fin}})$.

$\underline{\mathbf{V}(x, \pi)}$:

1. Parse $\boldsymbol{x}$ as $(z_{final}, C, \mathsf{V})$, π as $(\mathsf{acc}, \pi_{\mathsf{fin}})$.
2. If $\not{\ell}(z_{final}, \mathsf{V}) = \mathsf{reject}$ output reject.
3. Let $\boldsymbol{x} := (\mathsf{acc}, z_{final}, C, \mathsf{V})$.
4. Return $\mathbf{V}_{\mathsf{fin}}(\boldsymbol{x}, \pi_{\mathsf{fin}})$.

Theorem 8.1. *Let $\mathcal{R}_{F,\ell}$ be a trivial RCG relation. Then $(\mathbf{P}, \mathbf{V})$ is a zk-SNARK for $\mathcal{R}_{F,\ell}$.*

Proof. The main thing to prove is knowledge soundness. Let $\mathcal{A}$ be an algebraic adversary. We define the following extractor algorithm:

1. Given (x, π) - use the SNARK extractor to output $\omega = (\mathbf{w}\text{-}\mathsf{acc}, \mathsf{acc}, \mathsf{inst}, \pi^*)$.
2. Let $n := \mathsf{inst.count}$. Define $\mathsf{acc}_n := \mathsf{acc}, \mathsf{inst}_n := \mathsf{inst}$.
3. Now, for $i = n, \ldots, 1$:
   (a) If $\mathsf{acc}_i, \mathsf{inst}_i \in K$, let $\mathbf{w}\text{-}\mathsf{acc}_i, \boldsymbol{w}\text{-}\mathsf{inst}_i$ be the elements output by $\mathcal{A}$ such that $\mathsf{acc}_i = \mathsf{cm}(\mathbf{w}\text{-}\mathsf{acc}_i), \mathsf{inst}_i = \mathsf{cm}(\boldsymbol{w}\text{-}\mathsf{inst}_i)$.
   (b) Parse inst_i as $(z_i, \mathsf{count}_i, \hbar_i)$. Parse $\boldsymbol{w}\text{-}\mathsf{inst}_i$ as $(\mathsf{acc}'_i, \mathsf{acc}_{i-1}, \mathsf{inst}_{i-1}, w_i, \pi_i)$. Note that through this parsing we have in particular defined z_i, w_i and inst_{i-1}.

[3]We only need $\mathsf{cm}(\mathbf{w}\text{-}\mathsf{acc}_1)$ to be uniformly distributed over the image of cm. According to cm's structure, it may suffice to choose only a small subset of $\mathbf{w}\text{-}\mathsf{acc}_1$'s coordinates randomly, and set the rest to zero.

4. Define $z_0 := \mathsf{inst}_0.z$.

5. Output $w := (n, (z_0, \ldots, z_n), (w_1, \ldots, w_n))$.

Look at following n bad events. For some $i \in [n]$:

1. $\mathsf{acc}_i \notin K$, or $\mathsf{inst}_i \notin K$.

2. $\mathsf{acc}'_i \neq \mathsf{acc}_i$, or

3. $(\mathsf{inst}_i, \boldsymbol{w}\text{-}\mathsf{inst}_i) \notin \mathcal{R}$.

We first argue that if all of the above n events didn't happen $(x, w) \in \mathcal{R}_{F,\mathscr{f}}$: For each $i \in [n]$, $(\mathsf{inst}_i, \boldsymbol{w}\text{-}\mathsf{inst}_i) \in \mathcal{R}$ implies $F(z_{i-1}, w_i, z_i) = \mathsf{acc}$. Since $\mathsf{inst}_{i-1} = \boldsymbol{w}\text{-}\mathsf{inst}_i.\mathsf{inst}$, it also implies $\mathsf{inst}_{i-1}.\mathsf{count} = \mathsf{inst}_i.\mathsf{count} - 1$. So we have $\mathsf{inst}_1.\mathsf{count} = 1$. So $(\mathsf{inst}_1, \boldsymbol{w}\text{-}\mathsf{inst}_1) \in \mathcal{R}$ together with $\boldsymbol{w}\text{-}\mathsf{inst}_1.\mathsf{inst} = \mathsf{inst}_0$ implies $\mathsf{inst}_0.z.\mathsf{init} = \mathsf{true}$.

□

9 General Final predicate

Sketch: If we can end the IVC with a commitment S to the concatenation of the $\{S_i\}$ from all iterations. Then we can modify the final zk-SNARK in the last section to also check that $\mathscr{f}(S_1, \ldots, S_n) = \mathsf{accept}$.

For this purpose, instead of the F^* in section 5 we add protogalaxy constraints to obtain a commitment of the concatenation of the previous one with the S_i of this iteration.

Estimate of added prover complexity for concatenation constraints, using linearity.

Acknowledgements

References

[BC23] B. Bünz and B. Chen. Protostar: Generic efficient accumulation/folding for special sound protocols. *IACR Cryptol. ePrint Arch.*, page 620, 2023.

[BCCT12] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In *Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8-10, 2012*, pages 326–349, 2012.

[BCL+21] B. Bünz, A. Chiesa, W. Lin, P. Mishra, and N. Spooner. Proof-carrying data without succinct arguments. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 681–710. Springer, 2021.

[CT10] A. Chiesa and E. Tromer. Proof-carrying data and hearsay arguments from signature cards. In *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*, pages 310–331. Tsinghua University Press, 2010.

[Eag22] Liam Eagen. Bulletproofs++. *IACR Cryptol. ePrint Arch.*, page 510, 2022.

[FKL18] G. Fuchsbauer, E. Kiltz, and J. Loss. The algebraic group model and its applications. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, pages 33–62, 2018.

[GWC19] A. Gabizon, Z. J. Williamson, and O. Ciobotaru. PLONK: permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. *IACR Cryptology ePrint Archive*, 2019:953, 2019.

[KST21] A. Kothapalli, S. T. V. Setty, and I. Tzialla. Nova: Recursive zero-knowledge arguments from folding schemes. *IACR Cryptol. ePrint Arch.*, page 370, 2021.

[KZG10] A. Kate, G. M. Zaverucha, and I. Goldberg. Constant-size commitments to polynomials and their applications. pages 177–194, 2010.

[LS24] Hyeonbum Lee and Jae Hong Seo. On the security of nova recursive proof system. Cryptology ePrint Archive, Paper 2024/232, 2024. `https://eprint.iacr.org/2024/232`.

[Val08] P. Valiant. Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. In *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2008.