

stackproofs: Private proofs of stack and contract execution using PROTOGALAXY

August 3, 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. 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 "authorize" is not tied to one specific 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 While running, a contract can read, add or delete notes belonging to it. We can thus think of the notes as global variables shared between the different functions.

Let us think of all functions in this system as having multiple arguments, and returning **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 .

However, this doesn't yet deal with the notes. During native execution, note operations happened at a certain order. We can think of these operations as having timestamps incremented by one with each operation. We need to check, for example, that if a note was read in a certain timestamp, it was indeed created in an earlier timestamp. We can have the note operations - $\{add, read, delete\}$ - performed by a function be included in the public inputs of its circuit. 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 timestamp 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 allow 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? 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

mangrove, nexus, Jens’s talk.

2 Preliminaries

2.1 Terminology and Conventions

We assume our field \mathbb{F} is of prime order. We denote by $\mathbb{F}_{<d}[X]$ the set of univariate polynomials over \mathbb{F} of degree smaller than d . We assume all algorithms described receive as an implicit parameter the security parameter λ . Similarly, we assume all integer parameters in the paper are implicitly functions of λ .

Whenever we use the term *efficient*, we mean an algorithm running in time $\text{poly}(\lambda)$. 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 prime field of super-polynomial 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, i.e. write \mathbb{F} instead of $\mathbb{F}(\lambda)$. We write \mathbb{G} additively.

We often denote by $[n]$ the integers $\{1, \dots, n\}$. 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 $R : \mathbb{G} \rightarrow \mathbb{F}^2$. 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 $v \in \mathbb{F}$ is the *value*, and $c \in [M]$ is the *counter*. A *record operation* has one of the following forms:

- (add, v, c) ,
- (del, v, c_v, c) ,
- (read, v, c_v, c) .

Here $v \in \mathbb{F}$ is a value and $c, c_v \in [M]$ are counters. c is interpreted as the counter of the current operation. 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 c_v fields in all *del* operations $(\text{del}, v, c_v, c) \in \mathcal{O}$ are distinct.
3. If $(v, \text{read}, c_v, c) \in \mathcal{O}$, then $c_v < c$ and $(\text{add}, v, c_v) \in \mathcal{O}$.
4. If $(v, \text{del}, c_v, c) \in \mathcal{O}$ then $c_v < c$ and $(\text{add}, v, c_v) \in \mathcal{O}$.

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

- \mathcal{O} is consistent.
- $V = \{(v, c) | (\text{add}, v, c) \in \mathcal{O} \ \& \ \forall c' \in [M], (\text{del}, v, c, c') \notin \mathcal{O}\}$. 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 in the next section to 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 $G : \mathbb{F}^8 \rightarrow \mathbb{F}$ that is an implicit parameter in the following definition of the relation \mathcal{R}_{app} .

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

- $\mathfrak{x} = (f, \text{args}, c, f_1, \text{args}_1, f_2, \text{args}_2, \mathcal{O})$ where $f, f_1, f_2 \in \mathbb{G}$, $\text{args} \in \mathbb{F}^4$, $c \in \{0, 1, 2\}$;
- $\mathfrak{w} = (w_f, \omega)$ where
 - $w_f = (S_1, \dots, S_4, q_1, \dots, q_4)$, where $S_j \in [|\mathfrak{x}| + N]^n$, $q_j \in \mathbb{F}^n$ for each $j \in [4]$
 - $\omega \in \mathbb{F}^N$

such that

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

$$G(q_{1,i}, \dots, q_{4,i}, x_{S_{1,i}}, \dots, x_{S_{4,i}}) = 0.$$

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

3.3 Valid execution trees

By an *exeuction 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 $n \in T$, its label $(\mathfrak{x}, \mathfrak{w})$ is in \mathcal{R}_{app} .
2. For each $n \in T$, let $(\mathfrak{x}, \mathfrak{w})$ be its label. Let $\mathfrak{x} = (f, \text{args}, c, f_1, \text{args}_1, f_2, \text{args}_2, \mathcal{O})$. Then
 - $f \in F$.
 - The number of its children is c .
 - For $i \in [c]$, let $(f^i, \text{args}^i, c^i, f_1^i, \text{args}_1^i, f_2^i, \text{args}_2^i, \mathcal{O}^i)$ denote the first component of n 's i 'th child's label. Then $f_i = f^i$ and $\text{args}_i = \text{args}^i$.
 - 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 r* if 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}_{exec} capturing knowledge of an execution of bounded length with a certain output set of records. \mathcal{R}_{exec} consists of the pairs (x_{exec}, w_{exec}) of the form

- $x_{\text{exec}} = (\mathbf{r}, C, \mathbf{V})$,
- $w_{\text{exec}} = (n, \mathbf{T})$,

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

4 Repeated Computation with Global state

An RCG relation is defined by a pair of functions (F, f) .

We call $F(Z, W, S, Z^*) \rightarrow \{\text{accept}, \text{reject}\}$ the *transition predicate*.

We informally think of

- Z^* as the output of F (although the actual output is $\{\text{accept}, \text{reject}\}$).
- Z as the public input and W as the private input of F .
- 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, \mathbf{V} respectively. f is a function $f : D_1^* \times D_2 \rightarrow \{\text{accept}, \text{reject}\}$ called the *final predicate*.

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

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

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 $F(Z, W, Z^*, S) \rightarrow \{\text{accept}, \text{reject}\}$ as follows.

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

- S is a set of record operations.

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

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

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

In the lemma below, we denote by g_{empty} the empty stack.

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

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

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

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

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

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

4.2 Removing the global state

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

Claim 4.2. *Assume \mathbb{F} has characteristic larger than $n + 1$. Let \mathbf{V} be a set of records and $\mathcal{O} = \{(\text{op}_i, v_i, \text{vc}_i, c_i)\}_{i \in [n]}$ be a set of record operations (defining $\text{vc}_i = 0$ when $\text{op}_i = \text{add}$). Then \mathcal{O} has output \mathbf{V} if and only if the following rational function identities hold:*

1.

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

2. For some $m \in \mathbb{F}^n$, we have

$$\sum_{i \in [n], op_i = \text{add}} \frac{m_i}{X + v_i Y + c_i} = \sum_{i \in [n], op_i = \text{read}} \frac{1}{X + v_i Y + v c_i}.$$

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 \mathbf{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 \mathbf{V} means one of the following occurs.

1. The multi-set of counters $\{c_i\}_{i \in [n]}$ doesn't equal $\{1, \dots, n\}$. 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 , $(\text{del}, v, vc, c) \in \mathcal{O}$ but $(\text{add}, v, vc) \notin \mathcal{O}$; or for some $v, vc, c_1 \neq c_2$, $(\text{del}, v, vc, c_1), (\text{del}, v, vc, c_2) \in \mathcal{O}$: In the first identity RHS, we will have $M_{v,vc}$ with coefficient in the range $\{-1, \dots, -n\}$, while in the LHS it has coefficient one or zero.
3. \mathbf{V} is *not* equal to the set \mathbf{V}' of (v,c) for which $(\text{add}, v, c) \in \mathcal{O}$ but $(\text{del}, v, c) \notin \mathcal{O}$. We look at the first identity. \mathbf{V}' is precisely the set of (v,c) with coefficient one on the RHS, while \mathbf{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 , $(\text{read}, v, vc, c) \in \mathcal{O}$ but $(\text{add}, v, vc) \notin \mathcal{O}$: In the second identity RHS $M_{v,c}$ will have a coefficient in the range $\{1, \dots, n\}$ while in the LHS it has coefficient zero.

□

We reduce the relation $\mathcal{R}_{F,f}$ from the last section to \mathcal{R}_{F^*,f^*} :

Let F denote the function $F(Z, W, Z^*, S) \rightarrow \{\text{accept}, \text{reject}\}$ as from Section 4.1.

Define the function $F^* : (Z, W, Z^*) \rightarrow \{\text{accept}, \text{reject}\}$:

- $Z = (Z_F, h, \mathcal{s}, \alpha, \beta, \epsilon)$.
- $Z^* = (Z_F^*, h^*, \mathcal{s}^*, \alpha^*, \beta^*, \epsilon^*)$.
- $W = (W_F, S_F, M)$

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

1. $F(Z_F, W_F, S_F, Z_F^*) = \text{accept}$.
2. Let $S_F = \{(op_i, v_i, vc_i, c_i)\}_{i \in [m]}$. We have
 $\mathcal{s}^* = \mathcal{s} +$

$$\sum_{i \in [m]; op_i = \text{add}} \frac{1 + \epsilon m_i}{\alpha + \beta v_i + c_i} - \sum_{i \in [m]; op_i = \text{read}} \frac{\epsilon}{\alpha + \beta v_i + vc_i} - \sum_{i \in [m]; op_i = \text{del}} \frac{1}{\alpha + \beta v_i + vc_i} + \sum_{i \in [m]} \frac{\epsilon^2}{\alpha + c_i}.$$

$$3. \alpha^* = \alpha, \beta^* = \beta, \epsilon^* = \epsilon.$$

$$4. h^* = \mathcal{H}(h, \text{cm}(S_F, M))$$

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

1. $\mathcal{s} = \sum_{(v,c) \in V} \frac{1}{\alpha + \beta v + c} + \sum_{i \in [n]} \frac{\epsilon^2}{\alpha + c_i}$
2. $\mathcal{H}(h, V) = (\alpha, \beta, \epsilon)$

Lemma 4.3. *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 $n \leq C$. Fix some $\alpha, \beta, \epsilon \in \mathbb{F}$ and set of records V . Define $z_{\text{final}} = (\text{empty}, \mathbf{r}, \text{false})$, $z_{\text{final}}^* := (z_{\text{final}}, h, \mathcal{s}, \alpha, \beta, \epsilon)$ and set $\phi := (z_{\text{final}}^*, C, V)$. Assume the ZTA for the appropriate family of functions appearing in the proof. Suppose efficient \mathcal{A} outputs ω such that $(\phi, \omega) \in \mathcal{R}_{F^*, f^*}$.*

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 $(\mathcal{D}, \mathcal{H}, \text{cm}, n)$. Then e.w.p. $\text{negl}(\lambda)$, $((z_{\text{final}}, C, V), \varphi(\omega)) \in \mathcal{R}_{F, f}$.

Proof. Given a witness $\omega = (z', w')$ with $z' = (z'_0, \dots, z'_n)$, $w' = (w'_1, \dots, w'_n)$ output by \mathcal{A} , denote $z'_i = (z_i, h_i, \mathcal{s}_i, \alpha_i, \beta_i, \epsilon_i)$, $w'_i = (w_i, s_i, M_i)$. Define $\omega = \varphi(\omega)$ as $\omega := (z_0, \dots, z_n), (w_1, \dots, w_n), (s_1, \dots, s_n)$. From $(\phi, \omega) \in \mathcal{R}_{F^*, f^*}$, we know ω satisfies the transition constraints, namely for $i \in [n]$, $F(z_{i-1}, w_i, s_i, z_i) = \text{accept}$. We also know that $n \leq C$. It is left to show that e.w.p. $\text{negl}(\lambda)$ $f(z_{\text{final}}, V) = \text{accept}$. Sketch: From $((z_{\text{final}}^*, C, V), \omega) \in \mathcal{R}_{F^*, f^*}$ we know the equations from Claim 4.2 hold at α, β, ϵ . If they don't hold identically for ω can contradict ZTA. \square

5 Non-interactive folding schemes

We fix a vector space K over \mathbb{F} , and an \mathbb{F} -linear function $\text{cm} : \mathbb{F}^M \rightarrow K$, that will be an implicit parameter in the following definition.

Definition 5.1. Fix relations \mathcal{R} and \mathcal{R}_{acc} . An $(\mathcal{R} \mapsto \mathcal{R}_{\text{acc}})$ -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 $(\Phi, \omega) \in \mathcal{R}_{\text{acc}}$, $(\phi', \omega') \in \mathcal{R}$, and $\mathbf{P}(\Phi, \phi'; \omega, \omega') = (\pi, \Phi^*, \omega^*)$ then with probability $1 - \text{negl}(\lambda)$, $(\Phi^*, \omega^*) \in \mathcal{R}_{\text{acc}}$ and $\mathbf{V}(\Phi, \phi', \Phi^*, \pi) = \text{accept}$.
 - (b) **Knowledge soundness in the Algebraic Group Model:**
For any efficient \mathcal{A} the probability of the following event is $\text{negl}(\lambda)$: \mathcal{A} outputs $(\phi, \tau), \phi', (\phi^*, \tau^*), \omega, \omega', \omega^*, \pi$ such that
 - i. $\text{cm}(\omega) = \phi, \text{cm}(\omega') = \phi', \text{cm}(\omega^*) = \phi^*$,
 - ii. $\mathbf{V}(\phi, \phi', \phi^*, \pi) = \text{accept}$,
 - iii. $((\phi^*, \tau^*), \omega^*) \in \mathcal{R}_{\text{acc}}$,
 - iv. $((\phi, \tau), \omega) \notin \mathcal{R}_{\text{acc}}$ or $(\phi', \omega') \notin \mathcal{R}$.

5.1 Relations for folding schemes

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

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

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

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

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

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

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

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

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

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

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

5.2 The PROTOGALAXY scheme

Deviating from [?], we explicitly present PROTOGALAXY as a *non-interactive* folding scheme, 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}^* .

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

1. Compute $\delta = \mathcal{H}(\Phi, \phi_1)$. Define $\delta := (\delta, \delta^2, \dots, \delta^{2^{t-1}}) \in \mathbb{F}^t$.
2. Compute the polynomial

$$F(X) := \sum_{i \in [n]} \text{pow}_i(\beta + X\delta) f_i(\omega).$$

(Note that $F(0) = \sum_{i \in [n]} \text{pow}_i(\beta) f_i(\omega) = e$.)

3. Denote the non-constant coefficients of F by $a := (F_1, \dots, F_t)$.
4. Compute $\alpha = \mathcal{H}(\Phi, \phi_1, a)$.
5. Compute $\beta^* \in \mathbb{F}^t$ where $\beta_i^* := \beta_i + \alpha \cdot \delta_i$.
6. Define the polynomial $G(X)$ as

$$G(X) := \sum_{i \in [n]} \text{pow}_i(\beta^*) f_i(X \cdot \omega + (1 - X)\omega_1).$$

7. Compute the polynomial $K(X)$ such that

$$G(X) = F(\alpha)X + Z(X)K(X).$$

8. Let $b := (K_0, \dots, K_{d-2})$ 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 $\Phi^* = (\phi^*, \beta^*, e^*)$, where

$$\phi^* := \gamma \cdot \phi + (1 - \gamma)\phi_1,$$

- the witness $\omega^* := \gamma \cdot \omega + (1 - \gamma) \cdot \omega_1$,
- and the proof $\pi := (a, b)$.

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

1. Compute $\delta, \alpha, \beta^*, \gamma$ as in the prover algorithm given Φ, ϕ_1, a, b .
2. 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 5.2. Fix $\mathbf{cm} : \mathbb{F}^M \rightarrow K$, 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 $(\mathcal{D}, \mathcal{H}, \mathbf{cm})$ 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 $z := \mathcal{H}(\mathbf{cm}(x), \tau)$, we have $f(z) = 0$.

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

Theorem 5.3. Set $d' := \max\{n, d\}$. Denote $\mathbf{cm}'((\omega, \beta, e), \omega_1) := ((\mathbf{cm}(\omega), \beta, e), \mathbf{cm}(\omega_1))$. Let \mathcal{D} be a family of four functions to be defined in the proof. Assume that \mathbf{cm} is collision resistant and the ZTA holds for $(\mathcal{D}, \mathcal{H}, \mathbf{cm}', d')$. Then **PROTOGALAXY** is a $(\mathcal{R} \mapsto \mathcal{R}^{\text{rand}})$ -folding scheme.

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

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

According to Definition 5.1, knowledge soundness is equivalent to E having probability $\text{negl}(\lambda)$ 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}, cm) . By the theorem assumption this implies E is contained in two events of probability $\text{negl}(\lambda)$, and must have probability $\text{negl}(\lambda)$ itself.

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

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

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 $a = (a_1, \dots, a_t), b = (b_0, \dots, b_{d-2})$. 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 $\delta, \beta, \alpha, \beta^*, \gamma$ be computed as in the prover description given a, b . Define the polynomials

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

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

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

Set $x := ((\omega, \beta, e), \omega_1)$ 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

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

Define the polynomial $A(X) := \sum_{i \in [n]} f_i(\omega_1) \text{pow}_i(\beta_1 + X\delta, \beta_2 + X\delta^2, \dots, \beta_t + X\delta^{2^{t-1}})$. 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

$$B(X, Y) := \sum_{i \in [n]} f_i(\omega_1) \text{pow}_i(\beta_1 + XY, \beta_2 + XY^2, \dots, \beta_t + XY^{2^{t-1}}).$$

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 $\left\{ \text{pow}_i(\beta_1 + XY, \beta_2 + XY^2, \dots, \beta_t + XY^{2^{t-1}}) \right\}_{i \in [n]}$ 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 $(\Phi, \omega) \notin \mathcal{R}^{\text{rand}}$. As we're still assuming $G' \equiv 0$, we have

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

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

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

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. \square

6 On protogalaxy

6.1 Introspective constraints

Constraints f_i on ω , simply low degree polynomials, but have the ability to refer to components of $\text{cm}(m_j)$ Function F should have “introspection” ability to look at commitments.

commitment function will output two representations of $\text{cm}(w)$ - in \mathbb{G} and in \mathbb{F} and or PI will include \mathbb{F} representation. which will then be part of w . \mathbf{V} will check representations match.

6.2 Proving PROTOgalaxy under zero-testing assumption

7 The Algebraic Group Model with recursive extraction

As in [FKL18], we assume when \mathcal{A} outputs $a \in \mathbb{G}$ it outputs a vector $c \in \mathbb{F}^n$ with $\langle c, \text{srs} \rangle = a$. We fix some mapping $G : \mathbb{F}^4 \rightarrow \mathbb{G} \cup \{*\}$. $*$ means the input doesn't correspond to \mathbb{G} element. We assume that this is the representation \mathcal{A} uses for elements of \mathbb{G} .

For our security proof, we require a notion of “recursive extraction” used by [LS24]: Specifically, we assume that if c output by \mathcal{A} along with a , thought of as $c \in (\mathbb{F}^4)^{n/4}$, contains an element c_i with $G(c_i) = a \in \mathbb{G}$, then \mathcal{A} outputs $c' \in \mathbb{F}^n$ with $\langle c', \text{srs} \rangle = c$. The same holds for c' . Thus \mathcal{A} must continue outputting representations until reaching one where no element corresponds to $a \in \mathbb{G}$.

8 Extending the transition function to include the folding constraints

As in [KST21, BCL⁺21], we describe an extended function F' that includes the folding verifier.

8.1 Describing F'

$$\mathbf{x} = (z, \text{count}, h)$$

- z - output for F
- count - counter of IVC step
- h - supposed hash of accumulator

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

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

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

1. $\mathcal{H}(\Phi^*) = h$.
2. $V_{PG}(\Phi, \mathbf{x}_0, \pi, \Phi^*) = \text{accept}$.
3. $\phi.h = \mathcal{H}(\Phi)$.

4. If $\text{count} > 0$:
 - (a) $\mathfrak{x}_0.\text{count} = \text{count} - 1$.
 - (b) $F(\text{false}, \mathfrak{x}_0.z, w, z) = \text{accept}$
5. If $\text{count} = 0$:
 - (a) $F(\text{true}, \mathfrak{x}_0.z, w, z) = \text{accept}$

We can describe the full prover for $\mathcal{R}_{F,f} \mathbf{P}(x, w)$

1. Let $x = (z_{\text{final}}, C, V)$, $w = (n, z = (z_0, \dots, z_n), w = (w_1 \dots, w_n), s = (s_1, \dots, s_n))$ such that
 2. Let Φ be a randomly chosen satisfiable accumulator. Namley, $X_1 = (\omega, \beta, e)$ where ω and β are chosen randomly And e is set to $e = \sum_{i \in [n]} \text{pow}_i(\beta) f_i(\omega)$. 2. Let $x_1 = (z_1, G, 0, \text{hash}(\text{acc}_{\text{empty}}))$, $w_1 = (\text{acc}_{\text{empty}}, \text{acc}_{\text{empty}}, \text{inst}_0, \omega_0, \pi)$. Here inst_0 satisfied $\text{inst}_0.z = z_0$, and doesn't need to be a satisfiable instance.
 2. For each $i = 2..n$, compute $(X_i, W_i, \pi_i) = P_{PG}(X_{i-1}, W_{i-1}, x_{i-1}, w_{i-1})$ $x_i = (z_i, G, i-1, \text{hash}(X_i))$, $w_i = (X_i, X_{i-1}, x_{i-1}, \omega_{i-1}, \pi_i)$
 3. Output (X_n, W_n, x_n, w_n) .
- $V(G, z_{\text{final}}, (X, W, x, w))$: 1. Check that $(X, W) \in R_{\text{rand}}$, $(x, w) \in R$. 2. Check that $x.z = z_{\text{final}}$, $x.\text{acc} = X$, $x.G = G$, $x.\text{count} \leq C$.

Acknowledgements

References

- [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.

- [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.
- [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.