Anoma Research Topics | TECHNICAL REPORT

Rethinking VampIR

Anthony Hart[a]

[a]Heliax AG

* *E-Mail: anthony@heliax.dev*

Abstract

This paper provides an overview of VampIR v0.1.3 and outlines potential modifications for future versions. Specifically, it contains proposals for streamlined versions of the fresh function and constraint generation, a proposal for removing the type system, and a short proposal for dealing with imports. It ends with an overview of implementation improvements made in light of the Haskell port.

Keywords: VampIR; Arithmetic Circuits; Compilers; Proposals;

(Received July 31, 2023; Published: August 21, 2023; Version: August 29, 2023)

Contents

1. Introduction

VampIR serves as a language for constructing arithmetic circuits on finite fields (Heliax AG, 2023a), designed to be a universal intermediate language for numerous proof systems based on arithmetic circuits such as Halo2[1]. Higher-level languages, such as Juvix (Heliax AG, 2023b), which compile to arithmetic circuits, can employ VampIR as an intermediary.

The necessity for an intermediate language is evident. Without one, each desired proof system must be individually supported by the systems. However, with an adequate intermediate representation, the total workload required to establish the ecosystem remains linear. Languages can target the intermediate representation rather than a specific proof system, thereby gaining support for every proof system targeted by this intermediate representation.

VampIR aims to offer a minimal yet expressive interface for describing the core data structure utilized by most modern zero-knowledge proof systems. It is designed to be flexible and straightforward but does not incorporate any cryptographic features. VampIR files are sufficiently generic to be applicable for uses involving arithmetic circuits, even those unrelated to cryptography.

Here we focus on reevaluating the existing design of the VampIR front-end language and compiler. We present its syntax, type system, and semantics in Section 2 with the aim of proposing a more flexible design in Sections 3 and 4 for a new compiler with support for explicit constraints in modular VampIR programs as described in Sections 5 to 7.

$$
\begin{array}{rcll}
\text{VampIR} & ::= & \text{Arith} & \text{XXX} \\
& | & (\text{VampIR} \ = \ \text{VampIR}) & \\
& | & (\text{VampIR}; \ \text{VampIR}) & \\
& | & () & \text{XXX} \\
& | & (\text{VampIR}, \ \text{VampIR}) & \\
& | & \text{fst} \mid \text{snd} & \\
& | & \text{VampIR} :: \text{VampIR} \mid [] & \\
& | & \text{hd} \mid \text{tl} & \\
& | & \text{fresh VampIR}^{+} & \\
& | & \text{iter } n \text{ VampIR} & \\
& | & \text{fold VampIR VampIR VampIR} & \\
& | & \lambda v.\text{VampIR} & \\
& | & \text{VampIR VampIR} & \\
& | & \text{VampIR op VampIR} & \\
& | & -\text{VampIR} \mid f \mid v & \\
\text{op} & ::= & + \mid \times \mid - \mid / & \\
f & \in & \mathbb{F} & (\mathbb{F} \text{ is the field associated with the circuit.}) \\
\text{v} & \in & \text{string} &
\end{array}
$$

Fig. 1: VampIR syntax grammar.

2. Current VampIR

2.1. Syntax. If we retroactively turn VampIR into a calculus, then its syntax could be described as in Figure 8.

Remark 1. In Figure 8, VampIR^{+} is the same as VampIR, except for op which can also be $\%$ or $\div$, the non-field operations of modulus and integer division, respectively.

Remark 2. Note that real VampIR lacks the built-in operations fst, snd, hd, and tl operations. Instead, such operations are implemented via pattern matching; however, since pattern matching can only be done on tuples and lists, this ends up being equivalent to what we present here.

2.2. Type system. VampIR has a simple type system. The syntax of types can be defined as;

$$
\begin{array}{rcl}
\text{Type} & ::= & v \\
& | & \text{Type} \ \rightarrow \ \text{Type} \\
& | & \text{Type} \ \times \ \text{Type} \\
& | & [\text{Type}] \\
& | & () \\
& | & \mathbb{F}
\end{array}
$$

Fig. 2: VampIR types.

VampIR relies on a notion of first-order type for some determinations. The set of first-order types can be defined inductively following the grammar described in Figure 3.

$$
\begin{array}{rcl}
1st & ::= & () \\
& | & \mathbb{F} \\
& | & [1st] \\
& | & 1st \times 1st
\end{array}
$$

Fig. 3: First-order types.

The type-checking rules of VampIR are described in Figure 4.

[1] https://zcash.github.io/halo2/

$$\frac{x{:}T \quad y{:}U}{(x;\ y){:}U} \qquad \frac{f{\in}\mathbb{F}}{f{:}\mathbb{F}} \qquad \frac{\mathsf{op}{\in}\{+,*,-,/,\div,\%\} \quad x{:}\mathbb{F} \quad y{:}\mathbb{F}}{(x\ \mathsf{op}\ y){:}\mathbb{F}} \qquad \frac{T{\in}1st \quad x{:}T \quad y{:}T}{(x{=}y){:}()}$$

$$\frac{}{():()} \qquad \frac{x{:}T \quad y{:}U}{(x,y){:}T\times U} \qquad \frac{}{\mathsf{fst}{:}T\times U\to T} \qquad \frac{}{\mathsf{snd}{:}T\times U\to U} \qquad \frac{x{:}T\vdash y{:}U}{\lambda x.y{:}T\to U} \qquad \frac{x{:}T\to U \quad y{:}T}{(x\ \ y){:}U}$$

$$\frac{}{[]{:}[T]} \qquad \frac{x{:}T \quad l{:}[T]}{(x{::}l){:}[T]} \qquad \frac{}{\mathsf{hd}{:}[T]\to T} \qquad \frac{}{\mathsf{tl}{:}[T]\to[T]} \qquad \frac{}{\mathsf{fold}{:}U\to(T\to U\to U)\to[T]\to U}$$

$$\frac{n{\in}\mathbb{N}}{\mathsf{iter}\ \ n{:}T\to(T\to T)\to T}$$

Fig. 4: VampIR typing rules. Variables T and U are types as in Figure 2.

The types of free variables can vary, but each must have a unique type. VampIR requires that the type of a variable be inferable from context. For example, $(x = 1)$ allow us to infer that $x : \mathbb{F}$. Such variables always represent (tuples or lists of) public and/or private variables. The variables that represent tuples are further broken down. For example, if x is known to be a tuple, it can be divided into $(x.1, x.2)$, with $x.1$ and $x.2$ being new variable names. This process of splitting will continue until all variables are field elements. Note that a free variable cannot be a function; it has to be a first-order type, see Figure 3.

Remark 3. We use the typing rules described in Figure 4 to prevent many ill-formed terms. However, these rules do not prevent us from introducing expressions such as `hd []`. This will cause an error during evaluation.

2.3. Evaluation. The evaluation semantics is described in Figure 5 and is designed to have side effects that make it less intuitive than it would otherwise. During the evaluation, there is a global stack of constraints, denoted by χ below.

The correctness of evaluation requires the term to be well-typed, assuming that, for example, top-level VampIR program has type $()$. Missing patterns from the evaluation are, in a large way, eliminated by type checking.

$$\begin{array}{lcll}
[\![()]\!] & :\equiv & () & \\
[\![\mathsf{iter}\ (n+1)\ f\ x]\!] & :\equiv & [\![f\ (\mathsf{iter}\ n\ f\ x)]\!] & \\
[\![(x;y)]\!] & :\equiv & [\![x]\!];[\![y]\!] & \\
[\![(x,y)]\!] & :\equiv & ([\![x]\!],[\![y]\!]) & \\
[\![\mathsf{fst}\ (x,\ y)]\!] & :\equiv & [\![x]\!] & \\
[\![\mathsf{snd}\ (x,\ y)]\!] & :\equiv & [\![y]\!] & \\
[\![\mathsf{iter}\ 0\ f\ x]\!] & :\equiv & [\![x]\!] & \\
[\![(x::l)]\!] & :\equiv & ([\![x]\!]::[\![l]\!]) & \\
[\![\mathsf{hd}\ (x::l)]\!] & :\equiv & [\![x]\!] & \\
[\![\mathsf{tl}\ (x::l)]\!] & :\equiv & [\![l]\!] & \\
[\![\mathsf{fold}\ n\ f\ []]\!] & :\equiv & [\![n]\!] & \\
[\![\mathsf{fold}\ n\ f\ (x::l)]\!] & :\equiv & [\![n\ x\ (\mathsf{fold}\ n\ f\ l)]\!] & \\
[\![(p,\ q)=(r,\ s)]\!] & :\equiv & [\![p=r]\!];[\![q=s]\!] & \\
[\![(x::l)=(y::l')]\!] & :\equiv & [\![x=y]\!];[\![l=l']\!] & \\
[\![x=y]\!] & :\equiv & [\![\,[\![x]\!]=[\![y]\!]\,]\!], & (x,y:1st, \text{but not } x,y:\mathbb{F}) \\
[\![x=y]\!] & :\equiv & () & ([\![x]\!]=[\![y]\!] \text{ gets pushed onto } \chi, \text{ where } x,y:\mathbb{F}) \\
[\![(\lambda x.f)y]\!] & :\equiv & [\![\,f[y/x]\,]\!] & \\
[\![x\ \mathsf{op}\ y]\!] & :\equiv & r & (x,y\in\mathbb{F}, \text{and } r \text{ is the obvious result}) \\
[\![\mathsf{fresh}\ x]\!] & :\equiv & v & (v \text{ is a fresh variable})
\end{array}$$

Fig. 5: VampIR evaluation semantics.

Some things never need to be evaluated; for example, an unapplied lambda expression on its own should never occur during the evaluation of a well-formed program, so it does not need to be considered. Any unconsidered pattern should produce an error, although most such forms are already eliminated by type checking.

The nature of evaluation makes semantics somewhat nonintuitive. As a program is evaluated, it will output more and more constraints. There is no control over the constraints themselves as they are not manipulable objects of the language. Through the ability to ignore function calls, it is possible to prevent constraints from propagating (e.g. any constraint produced by `f` in `iter 0 f x`), but it is not always obvious when this will happen. The overall meaning of a program will be that, for a fixed set of public variables, there exists an assignment to the private variables such that the conjunction of all the constraints in χ is true.

Remark 4. The evaluation process generates a global stack of constraints, denoted as χ, through side effects, resulting in semantics that are not immediately compositional. However, due to the monoidal nature of conjunction, which makes the order of evaluation irrelevant, it is possible that compositional semantics could be recovered. Nevertheless, such semantics are not readily evident within the evaluation model.

3. Proposal: Remove the type system

The current type system in VampIR has led to limitations and the need for workarounds. While it is not inherently flawed, there is potential for a more versatile design. A key constraint is the inability to represent certain recursive programs due to typechecking. While solutions have been made to address specific instances, like lists and numbers, these are band-aid solutions that do not address the core issue: the limitations inherent in the type system itself.

While lists could be implemented using lambda expressions if removed from the language, their destructors, such as the head and tail, cannot be iterated due to typechecking issues. This requires the addition of built-in lists and accompanying `hd`, `tl`, and `fold` functions. A similar limitation arises with natural numbers; these numbers could also be lambda encoded, but iterated predecessors do not type check, limiting their usage. `iter` was added to compensate; it just interprets its natural number argument as a church numeral; something that can already easily be implemented.

The same issue arises with any recursive type. For example, binary trees can be lambda encoded, and, in fact, one can fold over them as well already in VampIR. One can even take the left and right branches, but iteration over these branches does not type check. Some version of this issue emerges with all recursive types. VampIR has no solution currently. The way things have been done in the past suggests extending the language, perhaps with a full-fledged recursive type system. However, we would prefer a different solution: remove the type system.

The type system does not prevent exponentially sized circuits from occurring; just infinitely sized ones. The way to dealing with exponentially sized circuits is straightforward –halt evaluation prematurely. This method should suffice for managing infinite circuits when they arise.

VampIR primarily serves as an intermediate language. This makes facilities that prevent the developer from shooting themselves in the foot less important than it might be. It is already the user's responsibility to make sure VampIR code is sensible; giving them the additional responsibility to make sure that the code does not loop infinitely is trivial in comparison. The logic errors that the simple type system prevents are, perhaps, not all trivial, but they are not substantial either. Given the simplicity of the type system, the guarantees it gives should be easy to keep track of by hand.

Using lambda encodings for all data structures would allow essentially all the faculties of functional programming to be made available; from data structures to complex mutually recursive algorithms. As it stands, the type system filters this into a less useful subset than end users might otherwise want to use.

4. Proposal: Remove DSL and make `fresh` simpler

The design of VampIR has an understated issue related to `fresh`. During evaluation, the body of `fresh` is discarded, but VampIR saves it as a method to determine the value of the newly generated variable. This design does not impact circuit semantics but serves as a convenience tool. Instead of users manually entering values for private variables, `fresh` provides automatic calculation instructions. To aid this, `fresh` utilizes a DSL, essentially an extended version of VampIR with additional operations, like modulus, which are not easily represented in arithmetic circuits. This enables `fresh` to compute values, with subsequent constraints verifying the accuracy of these values.

So, what is the problem? The fact that `fresh` uses a manually created DSL means that users cannot use arbitrary programs to calculate the values that need to be filled with `fresh`. This has led to much discussion as to how or whether this language should be extended. Two paths emerge: perpetual addition of new elements as they arise, or making the DSL computationally universal. However, both may not be viable solutions, as the correct value for a private variable may need to be supplied by an oracle that cannot be implemented in a VampIR program. A workaround is manual declaration and submission of a private variable at proof generation time. Yet, this raises the question of why a `fresh` need to exist at all. If it is a reasonable feature of convenience, can it be made better?

Considering this, we suggest the complete elimination of the DSL, allowing only `fresh` to store a name and signature.

Example 5. Consider the following as a typical example of `fresh` usage.

```
def bool x = { x*(x-1) = 0; x };

def range5 a = {
 def a0:a1:a2:a3:a4:[] =
   fresh (((a\1) % 2):((a\2) % 2):((a\4) % 2):((a\8) % 2) :((a\16) % 2):[]);
    def a0 = bool a0;
    def a1 = bool a1;
    def a2 = bool a2;
    def a3 = bool a3;
    def a4 = bool a4;
    a = a0 + 2*a1 + 4*a2 + 8*a3 + 16*a4;
    (a0, a1, a2, a3, a4, ())
};
```

Here, `fresh` is calculating a list of values, and those values are calculated using integer division and the modulus operation. The suggestion is that this be changed into something like in the following program.

```
def bool x = { x*(x-1) = 0; x };

def range5 a = {
    def a0:a1:a2:a3:a4:[] = fresh (range5_fr a);
    def a0 = bool a0;
    def a1 = bool a1;
    def a2 = bool a2;
    def a3 = bool a3;
    def a4 = bool a4;
    a = a0 + 2*a1 + 4*a2 + 8*a3 + 16*a4;
    (a0, a1, a2, a3, a4, ())
};
```

Upon compilation, we expect the program above generates a list of named signatures, each representing a function requiring implementation. This program will contain a signature named `range5_fr` that takes one argument and produces a list of five elements. The length may or may not be part of the signature, but the basic input and output types are.

Now, when proving a circuit, implementations for every function in the signature must also be provided. The exact form will depend on the language, but one can easily imagine implementing a function that takes a name and a list of arguments to compute the required output for the circuit in any language. The prove function would then essentially have an additional argument: a partial function of type `string * [int] -> [int]`.

For languages lacking higher-order function support, a more complex approach may be needed, but this should not be a show-stopper in any case. While this system may present less convenience for certain examples compared to the current one, it compensates by offering full flexibility and potential simplifications to the language. Requiring VampIR to lean more towards a library than it currently does, as seen in practice within the Taiga[2] framework for shielded transactions.

5. Proposal: Explicit constraints

The difficulty in VampIR's semantics stems from its non-compositional nature as discussed in Remark 4. To fix this, we propose adding a type of constraint to the language. Lambda expressions should not generate constraints; rather, they should return sets of constraints.

For simplicity, we propose a modified language, albeit omitting certain elements that may be desirable to retain.

$$
\begin{array}{rcl}
\text{VampIR} & ::= & \text{Arith} \\
& | & \text{VampIR} \ = \ \text{VampIR} \\
& | & \text{VampIR} \wedge \text{VampIR} \\
& | & \text{Type} \ \times \ \text{Type} \\
& | & \lambda v.\text{VampIR} \\
& | & \text{VampIR VampIR} \\
& | & \text{VampIR op VampIR} \\
& | & -\text{VampIR} \\
& | & f \\
& | & v \\
\text{op} & ::= & + \mid \times \mid - \mid / \\
f & \in & \mathbb{F} \\
\text{v} & \in & \text{string}
\end{array}
$$

Fig. 6: VampIR syntax grammar.

$$
\begin{array}{rcl}
\text{Type} & ::= & v \\
& | & \text{Type} \ \rightarrow \ \text{Type} \\
& | & \text{Type} \ \times \ \text{Type} \\
& | & \mathbb{B} \\
& | & \mathbb{F}
\end{array}
$$

Fig. 7: Modified VampIR syntax grammar.

With these in place, we can give a sensible interpretation to any program of type $\mathbb{B}$; it will be, essentially, a set of constraints.

[2] https://github.com/anoma/taiga

$$\frac{f \in \mathbb{F}}{f : \mathbb{F}} \qquad \frac{\mathsf{op} \in \{+, *, -, /, \div, \%\} \quad x : \mathbb{F} \quad y : \mathbb{F}}{(x \ \mathsf{op} \ y) : \mathbb{F}} \qquad \frac{T \in 1st \quad x : T \quad y : T}{(x = y) : \mathbb{B}} \qquad \frac{x : \mathbb{B} \quad y : \mathbb{B}}{x \wedge y : \mathbb{B}}$$

$$\frac{x : T \quad y : U}{(x, y) : T \times U} \qquad \frac{}{\mathsf{fst} : T \times U \to T} \qquad \frac{}{\mathsf{snd} : T \times U \to U} \qquad \frac{x : T \vdash y : U}{\lambda x \, . \, y : T \to U} \qquad \frac{x : T \to U \quad y : T}{(x \ y) : U}$$

Fig. 8: Modified VampIR typing rules.

$$\begin{aligned} [\![x = y]\!] &:\equiv \{x = y\} \\ [\![x \wedge y]\!] &:\equiv [\![x]\!] \cup [\![y]\!] \\ [\![(p, q) = (r, s)]\!] &:\equiv [\![p = r]\!] \cup [\![q = s]\!] \\ &\vdots \end{aligned}$$

Fig. 9: Evaluation semantics for VampIR with explicit constraints.

By having functions return an explicit set of constraints, we do not need to worry about procedural order, etc. This will make function types more complicated, but it will also make them more intuitive. For example.

```
def bool x = { x*(x-1) = 0; x };
```

In current VampIR this function has type $\mathbb{F} \to \mathbb{F}$, despite the fact that it has the side effect of generating a constraint. In my proposed change, this would become;

```
def bool x = { (x*(x-1) = 0, x) };
```

and have type $\mathbb{F} \to \mathbb{B} \times \mathbb{F}$. This changes later usage; an example of a range check would become;

```
def range5 a = {
    def a0:a1:a2:a3:a4:[] = [...];
    def (c0, a0) = bool a0;
    def (c1, a1) = bool a1;
    def (c2, a2) = bool a2;
    def (c3, a3) = bool a3;
    def (c4, a4) = bool a4;
    def c5 = (a = a0 + 2*a1 + 4*a2 + 8*a3 + 16*a4);
    (c0 & c1 & c2 & c3 & c4 & c5
    , (a0, a1, a2, a3, a4, ()) )
};
```

There are alternatives to this. This typical pattern is an instance of a state monad; it may be better to implement state monad combinators and assume all functions are under a (possibly trivial) constraint set. Function composition would union the produced states together, etc. This would be just as compositional, but it would be, perhaps, less tedious than what we presented here. We can, however, implement such combinators in VampIR already, so that may be unnecessary.

There are additional potential benefits to what we presented here. For many functions, it's not always obvious when one should do prefix constraint checks. In the case of bit-vector computations, if one does not know if the inputs are actually constrained to 0 and 1 then one needs to check this. If we already know this (maybe we already checked this with an earlier operation, and the output of this op is guaranteed to still be a bitvector by construction) then we don't need to add prefix checks. In the current version of VampIR this is handled by having multiple versions of the same function, one with checks and the other without. This modification allows one to ignore generated constraints, reducing the need for redundancy.

6. Proposal VampIR Imports

As it stands, VampIR does not currently support any kind of import system. This stems, largely, from the fact that simply combining two files will force the top-level constraints of both files to be combined. Despite this, most VampIR files consist mainly of reusable functions. VampIR should be modified to allow for imports. This would allow much better code reuse, allowing several files to, for example, import range checks rather than forcing each to re-implement them.

There are several ways this could be done. The simplest would be to simply ignore all top-level constraints for imports. We could also make a second file format that specifically only has definitions and no top-level constraints.

My preferred approach is this: There should be two kinds of VampIR files; one that has top-level constraints and another that contains only definitions. These should not be allowed to mix and match. This would prevent spurious constraints and would encourage programmers to abstract functionality into reusable definitions.

7. VampIR Haskell

Recently, a port of VampIR from Rust into Haskell was started. As part of this, many important implementation differences have been made. This section will briefly summarize them.

In the original implementation of VampIR, parsing was done through a PEG grammar. There was a .pest file which was then used to define a datatype in which parsed modules were stored. The Haskell implementation uses parser combinators as provided by the Megaparsec library. This significantly reduces the parsing code from over a thousand lines in Rust to less than 200 in Haskell. This is far more maintainable. In the original implementation of VampIR, there were periodic stack overflows when certain files were parsed; it is not clear at this point if the parser combinators will be more efficient in this respect.

The original version of VampIR parsed everything into the same format used for computation. The Haskell implementation has a separation between a simpler "core" language and a more complicated type representing VampIR ASTs. This allows things like pattern matching to be removed prior to evaluation or type checking. This also allows the core expressions to use higher-order abstract syntax, allowing us to reuse Haskell's binding features instead of implementing them anew.

In the original version of VampIR, all expression constructors were wrapped in a type annotation. These annotations were blank by default, and only filled during type checking. After type checking, these annotations were removed, but the wrappers themselves were always present. This made the language data types more complicated than necessary, and type annotations themselves are simply not necessary since VampIR's type system is simple enough that a most general type can always be efficiently inferred. The type checker in the Haskell implementation infers the most general type, and attempts unification to check for valid types.

In the original, compiled VampIR circuits came equipped with a large dictionary of definitions that told the system how to calculate intermediate circuit values. As an example, an expression like;

```
x + (y * z) = 2
```

would be turned into something like

```
x + v = 2
v = y * z
```

Additionally, separate from the actual circuit sent to Halo2 or Plonk, there would be a definition telling the system that v's value can be calculated by multiplying y and z. This is both obviously redundant and significantly complicates things like optimization as one needs to keep track of not just the circuit, but also ancillary definitions. The Haskell implementation uses constraint propagation to infer what values unassigned variables must take based on the 3ac constraints they are a part of. Any values which could have been inferred by simply evaluating the circuits can also be inferred like this, with no change in asymptotic efficiency. This would also significantly simplify any future optimization work, although the Haskell implementation currently does not do any optimization.

8. Acknowledgements

The original designs of VampIR are credited to X and Y.

References

Heliax AG. VampIR Rust Implementation, 2023a. URL https://github.com/anoma/vamp-ir/. (cit. on p. 1.)
Heliax AG. Juvix Compiler, 2023b. URL https://github.com/anoma/juvix/. (cit. on p. 1.)