Abstract
Secure multi-party computation (MPC) enables a set of mutually distrusting parties to cooperatively compute, using a cryptographic protocol, a function over their private data. This paper presents WYS*, a new domain-specific language (DSL) implementation for writing MPCs. WYS* is a Verified, Domain-Specific Integrated Language Extension (VDSILE), a new kind of embedded DSL hosted in F*, a full-featured, verification-oriented programming language. WYS* source programs are essentially F* programs written against an MPC library, meaning that the programmers can use F*’s logic to verify the correctness and security properties of their programs. To reason about the distributed semantics of these programs, we formalize a deep embedding of WYS*, also in F*. We mechanize the necessary metatheory to prove that the properties verified for the WYS* source programs carry over to a distributed, multi-party semantics. Finally, we use F*’s extraction mechanism to extract an interpreter that we have proved matches this semantics, yielding a verified implementation. With WYS* we have implemented several MPC protocols from the literature (including private set intersection and joint median) and have verified both their security and correctness.

1. Introduction
Secure multi-party computation (MPC) is a framework that enables two or more parties to compute a function $f$ over their private inputs $x_1, \ldots, x_n$ so that no party sees any of the others’ inputs, but rather only sees the output $f(x_1, \ldots, x_n)$. Utilizing a trusted third party to compute $f$ would achieve this goal, but in fact we can achieve it using one of a variety of cryptographic protocols carried out only among the participants [6, 18, 43, 49]. One example use of MPC is private set intersection (PSI): the $x_i$ could be individuals’ personal interests, and the function $f$ computes their intersection, revealing which interests the group has in common, but not any interests that they don’t. Among other applications, MPC has been used for auctions [13], detecting tax fraud [12], managing supply chains [24], and performing privacy preserving statistical analysis [23].

Typically, cryptographic protocols expect $f$ to be specified as a boolean or arithmetic circuit. Programming directly with circuits and cryptography via a host-language API is painful, so starting with the Fairplay project [31] many researchers have designed higher-level domain-specific languages (DSLs) in which to program MPCs [8, 11, 20, 21, 26, 29, 30, 35, 36, 39, 41, 46]. These DSLs compile normal looking code to circuits which are then given to the underlying protocol. While doing this undoubtedly makes it easier to program MPCs, these languages still have several drawbacks regarding both security and usability.

First, MPC participants should be able to reason that $f$ is sufficiently privacy preserving, i.e., that its output will not reveal too much information about the inputs [32]. The goal of an MPC DSL is secure computations, and such reasoning gives assurance that this goal is being achieved. Yet, only a few DSLs (Sharemind DSL [26], Wysteria [39], and SCVM [29]) have a mathematical semantics that can serve as a basis for formal reasoning.

Second, those languages that do have a semantics lack support for (semi-)automated reasoning of MPC programs: only by-hand proofs are possible, which provide less assurance than formally verified proofs. A middle ground might be a mechanization of the semantics and its metatheory [3], which adds greater assurance that it is correct [25], but no DSL has a mechanized semantics.

Third, there is a gap between the semantics, if there is one, and the actual implementation. Within that gap is the potential for security holes. Formal verification of the MPC DSL’s toolchain can significantly reduce the occurrence of security-threatening bugs [10, 28, 37, 47, 48], but no existing MPC DSL implementation has been (even partially) formally verified.

Finally, there is the practical problem that existing DSLs do not scale up, because they lack the infrastructure of a full-featured language. Adding more features (to both the language and the formalization) would help, but doing so quickly becomes unwieldy and frustrating, especially when the added features are “standard” and do not have much to do with MPC. We want access to libraries and frameworks for I/O, GUIs, etc. in a way that easily adds to functionality without adding complexity or compromising security.

This paper presents WYS*, a new MPC DSL that address these problems. WYS* is not a standalone language, but is rather what we call a Verified, Domain-Specific Integrated Language Extension (VDSILE), a new kind of embedded DSL that can be hosted by F* [44], a full-featured, verification-oriented programming language in the style of ML. WYS* is essentially an improved version of the Wysteria MPC DSL [39] implemented as a VDSILE.

A VDSILE is exemplified by three elements.

- Integrated language extension (Section 2). Programmers can write WYS* MPC source programs in what is essentially an extended dialect of F*. Like so-called shallow domain-specific language embeddings, the Wysteria-specific combinators are expressed in normal F* syntax, with prescriptions on their correct use expressed with F*’s dependent type-and-effect system. This arrangement means that programmers can use F*’s semi-automated verification facilities to prove properties about their MPC programs.

- Deep embedding of domain-specific semantics (Section 3). A shallow embedding implements the semantics of a DSL using the abstraction facilities of the host language, e.g., as a kind of library. However, for Wysteria this is impossible because its core semantics cannot be directly encoded in F*’s semantics. This is because a Wysteria program is like a kind of SIMD program in which many parties alternate between computing locally on their own data, in parallel, and computing jointly and securely on shared data. While such a program can be viewed as having a single
thread of control, it is not directly implemented that way. As such, we take the approach of a typical deep embedding: We define an interpreter in F* that operates over WYS* abstract syntax trees (ASTs), defined as an F* data type; these trees are produced by running the F* compiler (in a special mode) on the extended source program. Importantly, our interpreter does not need to understand all F* constructs that might be extracted. Even though their use is intermixed with Wysteria-specific constructs, their semantics is handled by a lightweight FFI, mostly hidden from the source programmer.

• Partially verified implementation (Sections 3 and 4). Within F* we mechanize two operational semantics for Wysteria: a single-threaded semantics that formalizes the SIMD view, mentioned above, and a distributed semantics, that formalizes programs as they are actually run by multiple parties. Importantly, we have machine-checked proofs that the single-threaded semantics is sound with respect to the distributed semantics, and that the distributed semantics is correctly implemented by our interpreter. As a result, we have verified that the properties we prove about the Wysteria-extended F* source programs hold for the multi-party programs that actually run. There is an important caveat, though: Our interpreter makes use of a circuit library to compile ASTs to circuits and then execute them using the Goldreich, Micali and Wigderson (GMW) multi-party computation protocol [18], but at present this library is not formally verified. Formal verification of GMW (which is, at present, an open problem) would add even greater assurance.

Using WYS* we have implemented several programs, including PSI, and joint median (Section 5). For PSI and joint median we implemented two versions each, a straightforward one, but which achieves poor performance, and a more optimized version. We formally proved that the optimized and unoptimized versions are equivalent, both functionally and with respect to privacy. In particular, our target semantics is “instrumented” with a trace of observations, and we prove that the visible events in the optimized version’s trace provides neither participant with any additional information about the other’s secrets. Performance experiments confirm that the optimized versions do indeed perform better.

In summary, this paper makes two main contributions:

- We propose Verified, Domain-Specific Integrated Language Extensions (VDSILE) as a new way to implement a domain-specific language. This approach provides a high degree of flexibility and ease of use, while adding the benefit of high assurance to the language implementation and programs written in it.

- We demonstrate the VDSILE approach on WYS*, an embedding of the Wysteria MPC DSL. The programs we have written with WYS* constitute the first MPC programs to be formally verified, and the WYS* implementation itself is the first MPC DSL to be be constructed with formal assurance. (Section 6 describes related work carefully.) Both the implementation and examples are publically available online on github, and are also included in the supplemental material.

2. Verified programming in WYS*

Consider a dating application that enables its users to compute their common interests without revealing all their private interests to one another. This is an instance of the private set intersection (PSI) problem. We illustrate the main concepts of WYS* by showing, in several stages, how to program, optimize, verify and deploy this application—Figure 1 provides an overview.

---

1 This is similar to what happens with C#’s language integrated queries (LINQ), but is a bit more flexible, as discussed in Section 6.
One obvious question is how both parties are able to get this process off the ground, running this program of four inputs, when only three of the inputs are known to them (the principals and their own input). In Wys', values specific to each principal are sealed with the principal's name (which appears in the sealed container's type). As such, the types of input_a and input_b are, respectively, list (sealed {a} int) and list (sealed {b} int). When the program is run on Alice's host, the former will be a list of n of Alice's values, whereas the latter will be a list of n garbage values (which we denote as ●). The reverse will be true on Bob's host. When the circuit is constructed, each principal links their non-garbage values to the relevant input wires of the circuit. Likewise, they populate a local copy of the output map with what is returned to them, mapping the other principals' outputs to ●.

We would like MPC's like psi to be called from normal F* programs. For example, we would like the logic for a dating application, which involves reading inputs, displaying results, etc. to be able to call into psi to compute common interests. To achieve this, Wys' provides a way to compute a "single-party projection" of multi-party functions, i.e., a version of psi that can be called with just a single party's inputs. The other party's inputs are filled in with sealed garbage values, as described above. Calling this function from F* code also kicks off the Wys' interpreter, so that it can run psi as described above. When the interpreter completes, the result is returned and the F* program can continue.

2.2 Optimizing PSI with as_par

Although psi gets the job done, it turns out to be inefficient (as shown in §5). Better implementations of PSI involve performing a mixed-mode computation, where each participant evaluates some local computations in parallel (e.g., iterating over the elements of their sets) interleaved with small amounts of jointly evaluated, cryptographically secure computations. Wys' second computation mode, called par mode, supports such mixed-mode computation. In particular, the construct as_par ps f states that each principal in ps should locally execute the thunk f, simultaneously (any principal not in the set ps simply skips the expression). Within f, principals may engage in secure computations via as_sec.

Below is an optimized version of PSI, based on an algorithm by Huang et al. [22], which uses as_par. The function psi_opt (line 12) begins by using as_par involving Alice and Bob. In the provided thunk, each principal calls for_each_alice la lb, which in turn calls check_each_bob a lb, for each element a of Alice's list la. Secure computation occurs at the use of as_sec at line 8. Within the circuit, Alice and Bob securely compare their values ax and bx, and gather a list (list bool), There is one outer list for each of Alice's elements, the ith inner list contains comparisons of Alice's ith value with some of Bob's values—rather than comparing each of Alice's elements with all of Bob's, the code is optimized (as described below) to omit redundant comparisons. At line 13, both parties build a matrix of comparisons from the boolean lists. Alice inspects the rows of the matrix (line 14) to determine which of her elements are in the intersection; Bob inspects the columns (line 15); and the joint function gives a result to each principal (line 16).

```
13 let bs = build_matrix (for_each_alice la lb) in
14 let ia = as_par {a} (fun () -> filteri (contains true o row bs) la) in
15 let lb = as_par {b} (fun () -> filteri (contains true o col bs) lb) in
16 give ia ++ give lb
```

The optimizations are at line 9. Once we detect that element ax in the intersection, we return immediately instead of comparing ax against the remaining elements of lb. Furthermore, we remove bx from lb, excluding it from any future comparisons with other elements of Alice's set la. Since la and lb are representations of sets (no repeats), all the excluded comparisons are guaranteed to be false.

One might wonder whether we could have programmed most of this code normal F*, relying on just sec mode for the circuit evaluation. However, recalling that our goal is to formally reason about the code and prove it correct and secure, par mode provides significant benefits. In particular, the SIMD model provided by Wys' enables us to capture many invariants for free. For example, proving the correctness of psi_opt requires reasoning that both participants iterate their loops in lock step—Wys' assures this by construction. Besides, the code would be harder to write (and read) if it were split across multiple functions or files. As a general guideline, we use F* for code written from the view of a single principal, and Wys' when programming for all principals at once, and rely on the FFI to mediate between the two.

2.3 Embedding a type system for Wys' in F*

Using the abstractions provided by Wysteria, designing various high-level, multi-party computation protocols is relatively easy. However, before deploying such protocols, three important questions arise. b

1. Is the protocol realizable? For example, does a computation that is claimed to be executed only by some principals ps (e.g., using an as_par ps or an as_sec ps) only ever access data belonging to ps?
2. Does the protocol correctly implement the desired functionality? For example, does it correctly compute the intersection of Alice and Bob's sets?
3. Is the protocol secure? For example, do the optimizations of the previous section that omit certain comparisons inadvertently also release information besides the final answer?

By embedding Wys' in F* and leveraging its type system, we address each of these three questions. Our strategy is to make use of F*'s extensible, monadic dependent type-and-effect system to define a new indexed monad (called Wys) and use it to describe precise trace properties of Wysteria multi-party computations. Additionally, we make use of an abstract type, sealed ps t, representing a value accessible only to the principals in ps. Combining the Wys monad with the sealed type, we encode a form of information-flow control to ensure that protocols are realizable.

The Wys monad provides several features. First, all DSL code is typed in this monad, encapsulating it from the rest of F*. Within the monad, computations and their specifications can make use of two kinds of ghost state: modes and traces. The mode of a computation indicates whether the computation is running in an as_par or in an as_sec context. The trace of a computation records the sequence and nesting structure of messages exchanged between parties as they jointly execute as_sec expressions—the result of a computation and its trace constitute its observable behavior. The Wys monad is, in essence, the product of a reader monad on modes and a writer monad on traces.

Formally, we define the following types of modes and traces. A mode Mode m ps is pair of a mode tag (either Par or Sec) and a set
of principals ps. A trace is a forest of trace element (telt) trees. The leaves of the trees record messages TMsg x that are received as the result of executing an as_sec block. The tree structure represented by the TScope ps t nodes record the set of principals that are able to observe the messages in the trace t.

type mtag = Par | Sec
type mode = Mode: m:mtag → ps:prins → mode
type telt =
| TMsg x:α → telt
| TScope ps:prins → t:list telt → telt

type trace = list telt

Every WYS* computation e has a monadic computation type Wys t pre post. The type indicates that e is in the Wys monad (so it may perform multi-party computations); t is its result type; pre is a pre-condition on the mode in which e may be executed; and post is a post-condition relating the computation’s mode, its result value, and its trace of observable events. When run in a context with mode m satisfying the pre-condition predicate pre m, e may send and receive message according to some trace tr, and if and when it returns, the result is a t-typed value v validating the post-condition predicate post m tr. The style of indexing a monad with a computation’s pre- and post-condition is a standard technique [2, 34, 44]—we defer the definition of the monad’s bind and return to the supplementary material and focus instead on specifications of combinators specific to WYS*.

We now describe two of the seven Wysteria-specific combinators in WYS*, as_sec and reveal, and how we give them types in P*.

**Defining as_sec in WYS***

1. val as_sec : ps:prins → f:unit → Wys a pre post) → Wys a
2. (requires (fun m → m:Mode Par ps ∧ pre (Mode Sec ps)))
3. (ensures (fun m r tr → tr= list TMsg r ∧ post (Mode Sec ps) r []))

The type of as_sec is dependent on the first parameter, ps. Its second argument f is the thunk to be evaluated in as_sec mode. The result’s computation type has the form Wys a (requires φ) (ensures ψ), for some pre-condition and post-condition predicates φ and ψ, respectively. The free variables in the type (a, pre and post) are implicitly universally quantified (at the front); we use the requires and ensures keywords for readability—they are not semantically significant.

The pre-condition of as_sec is a predicate on the mode m of the computation in whose context as_sec ps f is called. For all the ps to jointly execute f, we require all of them to transition to perform the as_sec ps f call simultaneously, i.e., the current mode must be Mode Par ps. We also require the pre-condition pre of f to be valid once the mode has transitioned to Mode Sec ps—line 2 says just this.

The post-condition of as_sec is a predicate relating the initial mode m, the result r a, and the trace tr of the computation. Line 3 states that the trace of a secure computation as_sec ps f is just a singleton [TMsg r], reflecting that its execution reveals only result r. Additionally, it ensures that the result r is related to the mode in which f is run (Mode Sec ps) and the empty trace [] (since f has no observations) according to post, the post-condition of f.

**Defining reveal in WYS*** As discussed earlier, a value v of type sealed ps t encapsulates a t value that can be accessed by calling reveal v. This call should only succeed under certain circumstances. For example, in par mode, Bob should not be able to reveal a value of type sealed {Alice} int. The type of reveal makes the access control rules clear:

![Image](https://example.com/image.png)

2This is the “ideal functionality” ensured by the backend, e.g., GMW.

---

val reveal: #ps:prins → x:sealed ps α → Wys α
  (requires (fun m → m:mode=Par ⊑ m.ps ≤ ps ∧ ModeSec =⇒ m.ps ∩ ps ≠ []))
  (ensures (fun m r tr → reveal a ∧ tr=[]))

This pre-condition says that when executing in Mode Par ps’, all current participants must be listed in the seal, i.e., ps’ ⊆ ps. However, when executing in Mode Sec ps’, only a subset of current participants is required: ps’ ∩ ps ≠ [] . This is because the secure computation is executed for all of ps’, so it can access any of their individual data.

### 2.4 Correctness and security verification

Using the Wys monad and the sealed type, we can write down precise types for our psi program, proving various useful properties. For lack of space, we discuss the statements of the main lemmas we prove and the proof structure—the details of their machine-checked proofs are left to the supplement. By programming the protocols using the high-level abstractions provided by WYS*, our proofs are relatively straightforward. In particular, we rely heavily on the view that both parties execute (different fragments of) the same code. In contrast, reasoning directly against the low-level message passing semantics would be much more unwieldy. In Section 3, by formalizing the connection between the high- and low-level semantics, we justify our source-level reasoning.

We present the structure of the security and correctness proof for psi_opt by showing the top-level specification for psi_opt:

val psi_opt : la:list (sealed Alice int) → lb:list (sealed Bob int) → Wys (map (Alice,Bob) (list int))
  (requires (fun m → m:Mode Par (Alice, Bob) ∧ no_dups la ∧ no_dups lb))
  (ensures (fun m r tr → let ia = as_set (Map.get r Alice) in
                let lb = as_set (Map.get r Bob) in
                ia = lb ∧ ia = (as_set la ∧ as_set lb) ∧ tr= psi_opt_trace la lb))

The signature above establishes that when Alice and Bob simultaneously execute psi_opt (they start together in Par mode), with lists la and lb containing their secrets (without any duplicates), then if and when the protocol terminates, they both obtain that same results ia and ib corresponding to the intersection of their sets, i.e., the protocol is functionally correct.

To prove properties beyond functional correctness, we also prove that the trace of observable events from a run of psi la lb is described by the function psi_opt_trace la lb. This is a purely specification-cational function that, in effect, records each of the boolean results of every as_sec comparison performed during a run of psi—it has the same structure as for each_alice and check_each_bob.

Given a full characterization of the observable behavior of psi_opt_trace la lb in terms of its inputs, we can prove optimizations correct using relational reasoning [9] and we can also prove security hyperproperties [15] by relating traces from multiple runs of the protocol.

Our goal is to prove a noninterference with delimited release [40] property for psi_opt. Our attacker model is the “honest-but-curious” model where the attackers are the participants in the protocol themselves. That is, we assume that the participants in the protocol play their roles faithfully, but they are motivated to deduce as much as they can about the other participants’ secrets by observing the protocol. We do not aim to prove security properties against a third-party network adversary.

For psi, from the perspective of Alice as the attacker, we aim prove that for two runs of the protocol in which Alice’s input is constant but Bob’s varies, Alice learns no more by observing the the protocol trace than what she is allowed to. Covering Bob’s perspective symmetrically, we show that in two runs of psi la0 lb0 and psi la1 lb1 that satisfy formula Ψ below, the traces observed
In the previous section, we presented examples of verifying properties do not reveal further information. First, we formalize the W property that we verify using F by showing that there exists a function psi e2 e1 creates a map from principals in e1 (which is a principal set) to the value computed by e2. project e1 e2 projects the value of principal e1 from the map e2, and concat e1 e2 concatenates the two maps.

Host language (i.e., F) constructs are also part of the syntax of WYS*, including constants e include strings, integers, lists, tuples, etc. Likewise, host language functions/primitives can be called from WYS*—i.e., f e is the invocation of a host-language function f with arguments e. The FFI confers two benefits. First, it simplifies the core language while still allowing full consideration of security relevant properties. Second, it helps the language scale by incorporating many of the standard features, libraries, etc. from the host language.

3. Single-threaded semantics

The ST semantics is a model of the F semantics and the WYS* API. The ST semantics defines a judgment C → C’ that represents a single step of an abstract machine. Here, C is a configuration M; X; L; T; e. This five-tuple consists of a mode M, a stack X, an environment L, a trace T, and an expression e. The syntax for these elements is given in Figure 3. The stack and environment are standard; the trace T and mode M were discussed in the previous section.

The ST semantics is formalized in the style of Heib and Felleisen [16], where the redex is chosen by (standard) evaluation contexts E, which prescribe left-to-right, call-by-value evaluation order. A few of the core rules are given in Figure 4. In essence, the semantics extends a standard reduction machinery for a call-by-value, lambda calculus (in direct correspondence with a pure fragment of F), with several Wysteria-specific constructs. We argue, by inspection, that the Wysteria-specific constructs are in 1-1 correspondence with their specifications in the Wys monad. Despite the "eyeball closeness", there is room for formal discrepancy between the ST semantics and its static model within F*’s Wys monad. We leave to future work formally proving a correspondence between the ST semantics and µF*, the official semantics of F* in F*

3 In carrying out this proof, it becomes evident that Alice and Bob learn the size of each other’s sets. One can compose psi_opt with other protocols to partially hide the size—WYS* makes it easy to compose protocols simply by composing their functions.

Figure 2. WYS* syntax

by Alice and Bob are indistinguishable, up to permutation, where la0, la1, lb0, lb1 have type iset int, the type of integer sets represented as lists.

ψ la0 la1 lb0 lb1 = intersec la0 lb0 intersect la1 lb1
∧ length la0 = length la1 ∧ length lb0 = length lb1

In other words, Alice and Bob learns no more than the intersection of their sets and the size of the other’s set; ψ is the predicate that delimits the information released by the protocol. As far as we are aware, this is the first formal proof of correctness and security of Huang et al.’s optimized, private set-intersection protocol.

The proof is in the style of a step-wise refinement, via psi, an inefficient variant of the psi_opt program. Running psi la lb always involves doing exactly length la + length lb comparisons in two nested loops. We prove the following relational security property for psi, relating the traces trace psi la0 lb0 and trace psi la1 lb1—the formal statement of the lemma we prove in F* is shown below.

val psi_is_secure: la1_→ lb1_→ la1_→ lb1_→ Lemma (requires (ψ la0 la1 lb0 lb1)) (ensures (permutation (trace psi la0 lb0) (trace psi la1 lb1)))

We reason about the traces of psi only up to permutation. Given that Alice has no prior knowledge of the choice of representation of Bob’s set (Bob can shuffle his list), the traces Alice observes are equivalent up to permutation—we can formalize this observation using a probabilistic, relational variant of F* [5], but have yet to do so.

As a next step, we prove that optimizing psi to psi_opt is secure by showing that there exists a function f, such that for any trace tr=trace psi la lb, the trace of psi_opt, trace psi_opt la lb, can be computed by f (length la) tr. In other words, the trace produced psi_opt la lb can be computed using a function of information already available to Alice (or Bob) when she (or he) observes a run of the secure, unoptimized version psi la lb. As such, the optimizations do not reveal further information.

3. Formalizing WYS*

In the previous section, we presented examples of verifying properties about WYS* programs using F*’s logic. However, these programs are not executed using the F* (single-threaded) semantics; instead they have a distributed semantics carried out by multiple parties. So, how do the properties that we verify using F* carry over to the actual protocol runs?

In this section, we present the metatheory that answers this question. First, we formalize the WYS single-threaded (ST) semantics, arguing that it faithfully realizes the F* semantics, including the WYS* API presented in Section 2. Next, we formalize the distributed (DS) semantics that the multiple parties use to run WYS* programs. Our theorems establish the correspondence between the two semantics, thereby ensuring that the properties that we verify using F* carry over to the actual protocol runs. We have mechanized all the metatheory presented in this section in F*.

WYS* programs. Our theorems establish the correspondence between the two semantics, thereby ensuring that the properties that we verify using F* carry over to the actual protocol runs. We have mechanized all the metatheory presented in this section in F*.

3.1 Syntax

Figure 2 shows the first-class syntax of WYS*. Principal and principal sets are first-class values, and are denoted by p and s respectively. Constants in the language also include (unit), booleans, and FFI constants e. Expressions e include the regular forms for functions, applications, let bindings, etc. and the WYS* specific constructs. Among the ones that we have not seen in Section 2, expression mkmap e1 e2 creates a map from principals in e1 (which is a principal set) to the value computed by e2. project e1 e2 projects the value of principal e1 from the map e2, and concat e1 e2 concatenates the two maps.

Host language (i.e., F) constructs are also part of the syntax of WYS*, including constants e include strings, integers, lists, tuples, etc. Likewise, host language functions/primitives can be called from WYS*—i.e., f e is the invocation of a host-language function f with arguments e. The FFI confers two benefits. First, it simplifies the core language while still allowing full consideration of security relevant properties. Second, it helps the language scale by incorporating many of the standard features, libraries, etc. from the host language.

3.2 Single-threaded semantics

The ST semantics is a model of the F* semantics and the WYS* API. The ST semantics defines a judgment C → C’ that represents a single step of an abstract machine. Here, C is a configuration M; X; L; T; e. This five-tuple consists of a mode M, a stack X, an environment L, a trace T, and an expression e. The syntax for these elements is given in Figure 3. The stack and environment are standard; the trace T and mode M were discussed in the previous section.

The ST semantics is formalized in the style of Heib and Felleisen [16], where the redex is chosen by (standard) evaluation contexts E, which prescribe left-to-right, call-by-value evaluation order. A few of the core rules are given in Figure 4. In essence, the semantics extends a standard reduction machinery for a call-by-value, lambda calculus (in direct correspondence with a pure fragment of F*), with several Wysteria-specific constructs. We argue, by inspection, that the Wysteria-specific constructs are in 1-1 correspondence with their specifications in the Wys monad. Despite the "eyeball closeness", there is room for formal discrepancy between the ST semantics and its static model within F*’s Wys monad. We leave to future work formally proving a correspondence between the ST semantics and µF*, the official semantics of F* in F* [44].

Figure 3. Runtime configuration syntax
The standard constructs such as let bindings (let \( x = e \) in \( e' \)), applications \((e_1 e_2)\), etc. evaluate as usual (see rules S-LET and S-APP), where the mode and traces play no role. Rules S-ASPAR and S-ASPARRET reduce an as-par expression once its arguments are fully evaluated. S-ASPAR first checks that the current mode is Par and contains all the principals from the set \( s \). It then pushes a seal \( \{ \} \) frame on the stack, and starts evaluating \( e \). The rule S-ASPARRET pops the frame and seals the result, so that it is accessible only to the principals in \( s \). The rule also creates a trace element TScope \( s \ T \), essentially making observations during the reduction of \( e \) (i.e., \( T \)) visible only to the principals in \( s \).

To see that these rules faithfully model the F\(^*\) API, consider the F\(^*\) type of as_par, shown below.

\[
\text{val as_par: ps:prins \rightarrow (unit \rightarrow Wys a pre post) \rightarrow Wys (sealed ps a)}
\]

\[
\begin{align*}
\text{(requires (fun m -> m.mode=Par \& \& ps \subseteq m.ps \& \\
\text{can_seal ps a \& pre (Mode Par ps)))} \\
\text{(ensures (fun m r tr \rightarrow \exists t: tr=[TScope ps t] \& \\
\text{post (Mode Par ps (unseal r t))}}} \\
\end{align*}
\]

Rule S-ASPAR implements the pre-condition on line 2. For the pre-condition on line 3, rule S-ASPARRET checks that the returned value can be sealed.\(^4\) The rule also generates a trace element TScope \( s \ T \), as per the post-condition on line 4, and returns the sealed value, as per the return type of the API and the post-condition on line 5.

Next consider the rules S-ASSEC and S-ASSECRET. Again, we can see that the rules implement the type of as_sec (shown in \( \S 2 \)). The rule S-ASSEC checks the pre-condition of the API, and the rule S-ASSECRET generates a trace observation TMsg \( v \), as per the post-condition of the API.

In a similar manner, we can easily see that the rule S-REVEAL implements the corresponding pre- and post-conditions as given in Section 2. The rule S-FFI implements the FFI call by calling a host-language function exec ffi. As expected, calling a host-language function has no effect on the Wys\(^*\)-specific state. Concretely, this is enforced by F\(^*\)'s monadic encapsulation of effects. The remaining rules are straightforward.

### 3.3 Distributed semantics

The DS semantics implements judgments of the form \( \pi \rightarrow \pi' \), where a protocol \( \pi \) is a tuple \((P, S)\) such that \( P \) maps each principal to its local configuration and \( S \) maps a set of principals to the configuration of an ongoing, secure computation. Both kinds of configurations (local and secure) have the form \( C \) (per Figure 3).

\(^4\) For technical reasons, function closures may not be sealed; see the technical report for details.

In the DS semantics, principals evaluate the same program locally and asynchronously until they reach a secure computation, at which point they synchronize to jointly perform the computation. This semantics is expressed with four rules, given in Figure 6, which state that either: (1) a principal can take a step in their local configuration, (2) a secure computation can take a step, (3) some principals can enter a new secure computation, and finally, (4) a secure computation can return the result to the (waiting) participants.

The first case is covered by rule P-PAR, which (nondeterministically) chooses a principal’s configuration and evaluates it according to the local evaluation judgment \( C \rightarrow C' \), which is given in Figure 5 (discussed below). The second case is covered by P-SEC, which evaluates using the ST semantics. The last two cases are covered by P-ENTER and P-EXIT, also discussed below.

**Local evaluation.** The rules in Figure 5 present the local evaluation semantics. These express how a single principal behaves while in par mode; as such, mode \( M \) will always be Par \( \{ p \} \). Local evaluation agrees with the ST semantics for the standard language constructs (not shown) and differs for Wys\(^*\)-specific constructs.\(^5\)

For an as_par expression, a principal either participates in the computation, or skips it. Rules L-ASPAR1 and L-ASPARRET handle the case when \( p \in s \), and so, the principal \( p \) participates in the computation. The rules closely mirror the corresponding ST semantics rules. One difference in the rule L-ASPARRET is that the trace \( T \) is not scoped. In the DS semantics, traces only contain TMsg elements; i.e., a trace is the (flat) list of secure computation outputs observed by that active principal. If \( p \notin s \), then the principal skips the computation with the result being a sealed value containing garbage \( \bullet \) (rule L-ASPAR2). The contents of the sealed value do not matter, since the principal will not be allowed to unseal the value anyway.

Rule L-SEAL has the same intuition as above. Rule L-REVEAL allows principal \( p \) to reveal the value sealed \( s v \), only if \( p \in s \). As should be the case, there are no local rules for as_sec—to perform a secure computation parties need to combine their data and jointly do the computation.

**Entering/exiting secure computations.** Returning to Figure 6, Rule P-ENTER handles the case when principals enter a secure computation. It requires that all the principals \( p \in s \) must have the expression form as_sec \( s (L_p, \lambda x.x.e) \), where \( L_p \) is their local environment associated with the closure. Each party’s local environment contains its secret values (in addition to some public val-

\(^5\) Our formal development actually shares the code for both sets of rules, using an extra flag to indicate whether a rule is “local” or “joint”.
uses). Conceptually, a secure computation combines these environments, thereby producing a joint view, and evaluates e under the combination. We define an auxiliary combine_v function on values as follows:

\[
\text{combine}_v(\bullet, v) = v \\
\text{combine}_v(v, \bullet) = v \\
\text{combine}_v(p, p) = p \\
\text{combine}_v(sealed v_1, sealed v_2) = sealed s (\text{combine}_v v_1 v_2)
\]

The first two rules handle the case when one of the values is garbage; in these cases, the function picks the other value. For sealed values, if the set s is the same, the function recursively combines the contents. The combine function for the environments combines the mappings pointwise. The combine functions for n values and environments is a folding of the corresponding function.

So now, consider the following code:

\[
\text{let } x = \text{as_par alice (fun } x \rightarrow 2) \text{ in} \\
\text{let } y = \text{as_par bob (fun } x \rightarrow 3) \text{ in} \\
\text{let } z = \text{as_sec alice, bob (fun } z \rightarrow (\text{unseal } x) + (\text{unseal } y)) \text{ in} ...
\]

In alice’s environment x will be mapped to sealed alice 2, whereas in bob’s environment it will be mapped to sealed alice \bullet. Similarly, in alice’s environment y will be mapped to sealed bob \bullet, whereas in bob’s environment it will be mapped to sealed bob 3. Before the secure computation, their environments will be combined, producing an environment with x mapped to sealed alice 2 and y mapped to sealed bob 3, and then, the secure computation function will be evaluated in this new environment.

Although the combine_v function as written is a partial function, our metatheory guarantees that at runtime, the function always succeeds. Since the principals are computing the same program over their view of the data, these views are structurally similar.

So, the rule P-ENTER combines the principals’ environments, and creates a new entry in the S map. The principals are now waiting for the secure computation to finish.

The rule P-EXIT applies when a secure computation has terminated and returns results to the waiting principals. If the secure computation terminates with value v, each principal gets the value slice_v p v. The slice_v function is analogous to combine_v, but in the opposite direction—it strips off the parts of v that are not accessible to p. Some cases for the slice_v function are:

\[
\text{slice}_v p p' = p' \\
\text{slice}_v p (\text{sealed } v) = \text{sealed } s \bullet, \text{ if } p \not\in s \\
\text{slice}_v p (\text{sealed } v) = \text{sealed } s (\text{slice}_v p v), \text{ if } p \in s
\]

As an example, consider the following code:

\[
\text{let } x = \text{as_sec (alice, bob) (fun } x \rightarrow \text{let } y = ... \text{ in } \text{alice } y) \]

Since the return value of the secure computation is sealed for alice, bob will get a sealed alice \bullet, produced using the slice_v function on the result of \text{alice } y.

In the rule P-EXIT, the \text{<} notation is defined as:

\[
M; X; L; T; \text{unseal } v \Rightarrow M; X; L; \text{concat } \text{TMsg } v; v
\]

That is, the returned value is also added to the principal’s trace to note their observation of the value.

3.4 Metatheory

Our goal is to show that the ST semantics faithfully represents the semantics of WYS* programs as they are executed by multiple parties, i.e., according to the DS semantics. We do this by proving \textit{simulation} of the ST semantics by the DS semantics, and by proving \textit{confluence} of the DS semantics.

\textbf{Simulation} We define a slice C function that returns the corresponding protocol \pi C for an ST configuration C. In the P component of \pi C, each principal p \in s is mapped to their slice of the protocol. For slicing values, we use the same \text{slice}_v function as before. Traces are sliced as follows:

\[
\text{slice}_v p (\text{TMsg } v) = [\text{TMsg } (\text{slice}_v p v)] \\
\text{slice}_v p (\text{TScope } s T) = \text{slice}_v p T, \text{ if } p \in s \\
\text{slice}_v p (\text{TScope } s T) = [], \text{ if } p \not\in s
\]

The slice of an expression (e.g., the source program) is itself. For all other components of C, slice functions are defined analogously.

We say that C is terminal if it is in Par mode and is fully reduced to a value (i.e., C.v is a value and C.X is empty). Similarly, a protocol \pi = (P, S) is terminal if S is empty and all the local configurations in P are terminal. The simulation theorem is then the following:

\textbf{Theorem 1} (Simulation of ST by DS). Let s be the set of all principals. If \text{C}_1 \rightarrow^* \text{C}_2, and \text{C}_2 is terminal, then there exists some derivation (\text{slice } s \text{C}_1) \rightarrow^* (\text{slice } s \text{C}_2) such that (\text{slice } s \text{C}_2) is terminal.

Notably, each principal’s value and trace in protocol (\text{slice } s \text{C}_2) is the slice of the value and trace in \text{C}_2.

\textbf{Confluence} We say that a protocol \pi strongly terminates in the terminal protocol \pi_t, written as \pi \Downarrow \pi_t, if all possible runs of \pi
terminate in some number of steps in $\pi_t$. Our confluence result then says:

**Theorem 2** (Confluence of DS). If $\pi \xrightarrow{\tau} \pi_1$, then $\pi \xrightarrow{\tau} \pi_t$.

Combining the two theorems, we get a corollary that establishes the soundness of the ST semantics w.r.t. the DS semantics:

**Corollary 1** (Soundness of ST semantics). Let $s$ be the set of all principals. If $C_1 \xrightarrow{\tau} C_2$, and $C_2$ is terminal, then $\langle \text{slice } s \ C_1 \rangle \xrightarrow{\tau} \langle \text{slice } s \ C_2 \rangle$.

Now suppose that for a Wys’s source program, we prove in $F^*$ a post-condition that the result is sealed alice $n$, for some $n > 0$. By the soundness of the ST semantics, we can conclude that when the program is run in the DS semantics, it may diverge, but if it terminates, alice’s output will also be sealed alice $n$, and for all other principals their outputs will be sealed alice $n$. Aside from the correspondence on results, our semantics also covers correspondence on traces. Thus, via our VDSILE embedding of Wysteria in $F^*$, the correctness and security properties that we prove about a Wys’s program using $F^*$’s logic, hold for the program that actually runs.

Of course, this statement is caveated by how we produce an actual implementation from the DS semantics; details are presented in the next section.

# 4. Implementation

This section describes our Wys interpreter. We have proved that the core of this interpreter implements our formal semantics, adding confidence that bugs have not been introduced in the translation from formalism to implementation.

## 4.1 Wys’s interpreter

The formal semantics presented in the prior section is mechanized as an inductive type in $F^*$. This style is useful for proving properties, but does not directly translate to an implementation. Therefore, we implement an interpretation function step in $F^*$ and prove that it corresponds to the rules; i.e., that for all input configurations $C$, step($C$) = $C'$ implies that $C$ $\xrightarrow{\tau}$ $C'$ according to the semantics. Then, the core of each principal’s implementation is an $F^*$ stub function tstep that repeatedly invokes step on the AST of the source program (produced by the $F^*$ extractor run in a custom mode), unless the AST is an as$_sec$ node. Functions step and tstep are extracted to OCaml by the standard process.

Local evaluation is not defined for as$_sec$, so the stub implements what amounts to P-ENTER and P-EXIT from Figure 6. When the stub notices the program has reached an as$_sec$ expression, it calls into a circuit library we have written that converts the AST of the second argument of as$_sec$ to a boolean circuit. This circuit and the encoded inputs are communicated to a co-located server, written using a library due to Choi et. al. [14] that implements the GMW MPC protocol. The server evaluates the circuit, coordinating with the GMW servers of the other principals, and sends back the result. The circuit library decodes the result and returns it to the stub. The stub then carries on with the local evaluation.

Our $F^*$ formalization of Wys’s is 5000 lines of code, including all the metatheory. It makes abundant use of $F^*$’s dependent types to state and prove invariants. The implementation of the (verified) step function is essentially a big switch-case on the current expression, and is 60 lines of code. The tstep stub is another 15 lines. The size of the circuit library, not including the GMW implementation, is 836 lines.

The stub, the implementation of GMW, the circuit library, and the $F^*$ extractor (including our custom Wys’s mode for it) are part of our trusted computing base. As such, bugs in them could constitute security holes. Verifying these components as well (especially the circuit library and the GMW implementation, which are open problems to our knowledge) is interesting future work.

## 4.2 FFI

When writing a source Wys program in $F^*$, the programmer can call functions from an FFI module. During compilation, the FFI module is extracted to OCaml using the regular $F^*$ extraction. The custom mode of the $F^*$ extraction that we have implemented, identifies the FFI calls in the Wys’s program, and extracts them to an $E_{ffi}$ AST form, which is part of the AST expression type.

\[
\text{type } \text{exp} = \ldots \\
| E_{ffi}: f_{\alpha} \to \text{list}\exp \to \text{inj}\beta \to \exp \\
| \text{unembed } V_{\text{unit}} = () \\
| \text{unembed } (V_{\text{list } \exp}s) = \nu ((\ast \text{values in the host language } \ast)) \\
| \text{unembed } (V_{\text{seal } s } \nu) = V_{\text{seal } s } \nu
\]

Interpreter specific values, such as $V_{\text{seal}}$, are passed as is. The FFI module does not have access to the Wys’s API in $F^*$, and hence it can only use these values parametrically. $E_{ffi}$ then calls the OCaml function $f$ with the un-embedded arguments. The OCaml function returns some result, that needs to be embedded back to the AST. So, the question is how can we embed the result at runtime? Inspecting the type of the result is not an option. The custom $F^*$ extraction mode comes to rescue.

When the extractor compiles an FFI call in the source program to an $E_{ffi}$ node, it has the type information for the return value of the FFI call. Using this information, it instruments the $E_{ffi}$ node with an injection, a function that can be used at runtime to embed the FFI call result back to the AST. For example, if the result is $(),$ the injection is (an OCaml function) $\text{fun } x \to V_{\text{unit}}.$ If the return value is an interpreter value (e.g. $V_{\text{seal}}$), the injection is the identity. If the return value is some host value (such as a list, tuple, or int), the injection creates an $V_{\text{node}}$ node. $E_{ffi}$ uses the injection to embed the result back to the AST, and returns it to the interpreter.

Our interface essentially provides a form of monomorphic, first-order interoperability between the (dynamically typed) interpreter and the host language. We do not foresee any problems extending our current work to higher order with coercions [19].

# 5. Applications

**Private set intersection.** We evaluate the performance of the $\psi$ (computing intersection in a single secure computation), and the $\psi_{opt}$ (the optimized version) algorithms from Section 2. The programs that we benchmark are slightly different than the ones presented there, in that the local col and row functions are not the verified ones. The results are shown in Figure 7. We measure the time (in seconds) for per party set sizes 96, 128, and 256, and intersection densities (i.e. the fraction of elements that are common) 0.5, 0.75, and 0.9.

The time taken by the unoptimized version is independent of the intersection density since it always compares all pairs of values. However, as the intersection density increases, the optimized

---

6 How $F^*$ programs call into Wys’s functions was described in Section 2.1.
version performs far better – it is able to skip many comparisons. For lower densities ($< 0.35$), the optimization does not improve performance, as the algorithm essentially becomes quadratic, and the setup cost for each secure computation takes over.

**Joint median.** We program unoptimized and optimized versions of the two-party joint median [38]. The programs take two distinct, sorted inputs from alice, \(x_1\) and \(x_2\), and two distinct, sorted inputs from bob, \(y_1\) and \(y_2\) and return the median of all four. In the unoptimized version, the whole computation takes place as a monolithic secure computation, whereas the optimized version breaks the computation, revealing some intermediate results, and off-loading some parts to the local hosts (much like PSI). We refer the reader to [38] for more details of the algorithms.

For both the versions, we prove functional correctness:

```hs
val median: 
\[\text{median}\,\text{Alice}(\text{int} \times \text{int}) \rightarrow \text{median}\,\text{Bob}(\text{int} \times \text{int}) \rightarrow \text{Wys}\,\text{int}\]
\begin{equation}
\begin{aligned}
\text{(requires } \text{fun } m \rightarrow m &= \text{Mode Par \{Alice, Bob\}}) \\
\text{(ensures } \text{fun } r t \rightarrow (\text{pre } \text{unseal } x) (\text{unseal } x) \implies \\
& r = \text{median spec } (\text{unseal } x) (\text{unseal } y)))
\end{aligned}
\end{equation}
```

where \text{median spec} is an idealized median specification. For the unoptimized version, we prove that the trace is \(\text{TMseq } r\), where \(r\) is the result of the computation, basically reflecting that the principals only see the final result. We prove the optimized version to be secure using a relational argument that the trace does not reveal more than the output.

**Other applications and secure server.** We have implemented some more applications in Wys*, including geo-location sharing and elements of mental poker. At the moment, we have only run these applications using a secure server back end. In this back end, \text{as sec} works by literally sending code and inputs to a separate server that implements the ST semantics directly. The server returns the result with a cryptographic proof of correctness to each party (we have verified the use of cryptography using a technique similar to Fournet et al. [17]). We conjecture that such a server could be useful for a trusted hardware based deployment scenario.

6. Related work

**Source program verification.** While the verification of the underlying crypto protocols has received some attention [1], the verification of the MPC source programs has remained largely unexplored. The only previous work that we know of is Backes et al. [4] who devised an applied pi-calculus based abstraction for MPC, and use it for formal verification. For an auction protocol that computes the min function, their abstraction comprises about 1400 lines of code. Wys* permits direct verification of higher-level MPC source programs and provides a verified toolchain.

**MPC DSL extensions.** As listed in the introduction, several MPC DSLs have been proposed in the literature [8, 11, 20, 21, 26, 29, 30, 35, 36, 39, 41, 46]. Most of these languages have standalone implementations, but like Wys*, a few are implemented as language extensions. Launchbury et al. [27] define a Haskell-embedded DSL for writing low-level “share protocols” on a multi-server “SMC machine”. OblivC [50] is an extension to C for two-party MPC that annotates variables and conditionals with an oblivious qualifier to identify private inputs; these programs are compiled by source-to-source translation. The former is essentially a shallow embedding, and the latter is compiler-based; Wys* is unique in its use of the VDSILE strategy.

**DSL implementation strategies.** DSLs are implemented in various ways, such as by developing a standalone compiler/interpreter, or by embedding the DSL (shallowly or deeply) in a host language. VDSILE’s language-integrated syntax bears relation to the approach taken in LINQ [33], which embeds a query language in normal C# programs, and implements these programs by extracting the query syntax tree and passing it to a provider to implement for a particular backend. Other researchers have embedded DSLs in verification-oriented host languages (e.g., Bedrock [7] in Coq [45]) to permit formal proofs of DSL programs, e.g. by embedding the DSL (shallowly or deeply) in a host language.

7. Conclusions

This paper has presented Wys*, a new MPC DSL based on the Wysteria DSL of Rastogi et al. [39], but implemented as a verified, domain-specific integrated language extension (VDSILE), which confers both higher assurance and greater flexibility to Wys’ MPC programs and to the underlying implementation.

**References**


