Robust and Compositional Verification of Object Capability Patterns

(Long Version)

DAVID SWASEY, MPI-SWS, Germany
DEEPAK GARG, MPI-SWS, Germany
DEREK DREYER, MPI-SWS, Germany

In scenarios such as web programming, where code is linked together from multiple sources, object capability patterns (OCPs) provide an essential safeguard, enabling programmers to protect the private state of their objects from corruption by unknown and untrusted code. However, the benefits of OCPs in terms of program verification have never been properly formalized. In this paper, building on the recently developed Iris framework for concurrent separation logic, we develop OCPL, the first program logic for compositionally specifying and verifying OCPs in a language with closures, mutable state, and concurrency. The key idea of OCPL is to account for the interface between verified and untrusted code by adopting a well-known idea from the literature on security protocol verification, namely robust safety. Programs that export only properly wrapped values to their environment can be proven robustly safe, meaning that their untrusted environment cannot violate their internal invariants. We use OCPL to give the first general, compositional, and machine-checked specs for several commonly-used OCPs—including the dynamic sealing, membrane, and caretaker patterns—which we then use to verify robust safety for representative client code. All our results are fully mechanized in the Coq proof assistant.

1 INTRODUCTION

Suppose you have a mutable reference \( \ell \) whose contents you care about, meaning that you want to impose some invariant on it (e.g., \( \ell \) always points to an even number). Suppose further that you want to share access to \( \ell \) with code you did not write and that you do not trust to preserve the invariant on \( \ell \). To ensure the invariant on \( \ell \) is maintained, you therefore do not want to pass the untrusted code the reference \( \ell \) directly. Instead, you might construct a read-only wrapper \( w \) as follows:

\[
\text{readonly} \triangleq \lambda r. \lambda _{\_} . \! r \quad w \triangleq \text{readonly} \ell
\]

Here, \textit{readonly} transforms a reference \( r \) into a thunk that, when applied, returns the current contents of \( r \). The expression \( w \) applies \textit{readonly} to our reference of interest \( \ell \), constructing a function for reading \( \ell \)'s contents. You can now pass \( w \) to untrusted code without worrying about it corrupting your invariant on \( \ell \).

Wrappers like \( w \) are often called object capabilities, and the wrapper construction function \textit{readonly} is a very simple example of an object capability pattern (OCP) [Miller et al. 2000]. Although OCPs date back at least to the 1970s [Morris 1973], they have gained increased currency in recent years, both in new languages centered around object capabilities [Miller et al. 2000; Mettlter et al. 2010; Spiessens and Roy 2004; Stiegler and Miller 2006] and in the context of web programming, where interfacing with untrusted code is commonplace. Web sandboxing systems like Yahoo!’s...
ADsafe [Crockford 2008; Politz et al. 2014] and Google’s Caja [Miller et al. 2008], for example, elaborate untrusted JavaScript source code into an ostensibly safe subset of JavaScript while introducing wrappers that attenuate access to JavaScript libraries. Caja relies on the so-called membrane pattern, which automatically wraps all objects crossing to untrusted, sandboxed code so that access to the underlying objects is appropriately restricted.

OCPs are believed to provide crucial security guarantees because, in a language like JavaScript, objects provide essentially no data abstraction on their own—the only way to enforce data abstraction is to hide private state in the environment of a closure (e.g., as $\ell$ was hidden in the environment of `readonly $\ell$` in the example above). So OCPs, which use closures to mediate access to private state in a systematic way, are one of the few effective mechanisms available in a language like JavaScript for enforcing data abstraction in the presence of possibly malicious code.

Unfortunately, despite the ubiquity of OCPs in modern web programming, remarkably little attention has been paid to the question of what exactly are the security guarantees that such OCPs are supposed to provide, and how might we prove that they actually provide them. Even in the case of the extremely basic `readonly` pattern shown above, it is not at all obvious what is the “right” formal specification for `readonly`. What, in particular, are the formal conditions on $\ell$ that are needed to guarantee that `readonly $\ell$` can be “safely” shared with untrusted code? If $\ell$ merely points to an integer, no conditions may be necessary, but what if $\ell$ points to a closure or some other higher-order object? How do we know that giving readonly access to $\ell$ will not indirectly give untrusted code a way of gaining full access and violating important invariants maintained by the user of this OCP?

The most recent, state-of-the-art attempt to grapple with these types of questions is due to Devriese et al. [2016]. They build a Kripke logical relations model for reasoning about object capabilities in a language with higher-order state, and they use their model to verify several concrete examples of capability-wrapped user code. In each case, they demonstrate that invariants on the private state of the user code are preserved even when the user code is shared with unknown attacker code. However, their model is limited in that it provides no way to compositionally specify what an OCP does, and it provides no clear specification of the general property that a piece of user code must satisfy in order to be safely shareable with untrusted code. Furthermore, they only consider very simple capability patterns, none as complex as, say, the aforementioned membrane pattern.

In this paper, we present OCPL (a Logic for OCPs), the first formal system for compositionally specifying and verifying the security guarantees provided by OCPs, in the context of a simple but representative programming language with higher-order functions, state, and concurrency.\(^1\) In contrast to prior work, OCPL enables one to reason modularly about both OCP implementations and user code that depends on them, and to specify a general property on user code that ensures such code can be safely shared with untrusted code without having its internal invariants violated. We use OCPL to reason about several commonly-used OCPs, including the dynamic sealing (sealer-unsealer), membrane, and caretaker patterns, and in so doing, provide the first formal explanation of what these OCPs achieve.

OCPL is a program logic derived from Iris, a recently developed framework for higher-order concurrent separation logic [Jung et al. 2015, 2016; Krebbers et al. 2017a]. Iris was originally proposed as a very general logic with a few simple primitives, using which one can derive advanced proof principles from a variety of modern separation logics as needed. Moreover, Krebbers et al. [2017b] have recently developed a powerful new proof mode for Iris in the Coq proof assistant. The Iris proof mode enables one to carry out interactive, tactical, machine-checked proofs about programs in the Iris logic (embedded in Coq) in much the same way as one normally carries out

\(^1\)Despite the name, object capabilities are not fundamentally limited to object-oriented programming languages.
Robust and Compositional Verification of Object Capability Patterns

interactive tactical proofs when working in the meta-logic of Coq itself. By virtue of building OCPL on top of Iris, we inherit the flexibility of the existing Iris framework, as well as its support for mechanizing proofs about programs in Coq. All our results and examples are, in fact, fully verified in Coq.

The key idea in OCPL is how it characterizes the interface between verified user code and untrusted code, via the concept of a “low-integrity value” (or low value for short) adapted from the literature on verification of security protocols [Abadi 1999]. Roughly speaking, a low value is a value that can be safely shared with untrusted code, such as the closure wrappers returned by OCPs. More precisely, a low value is a value from which no code can possibly extract a direct reference to private state. To formalize this notion, we employ a logical relation, which is easy to define using Iris’s built-in support for guarded recursive predicates. Then, with the idea of low values in hand, it becomes clear how to specify when a piece of user code can be safely linked with untrusted code—namely, when the only values passed back and forth between them are low values.

To make things concrete, let us return to our motivating example. Using the notion of low values, we can prove the following specification for the readonly pattern:

\[ \forall \ell. \{ \top \}\ !\ell \{ x. \text{lowval } x \} \Rightarrow \{ \top \} \text{readonly}\ell \{ f. \text{lowval } f \} \]

The premise of this spec says that, in order to apply readonly to a location \( \ell \), we must first prove that dereferencing \( \ell \) always produces a low value. (This makes sense because once we pass the read-only wrapper to untrusted code, it may invoke the wrapper and obtain the contents of \( \ell \) at any time.) The payoff is in the conclusion: the closure returned by readonly\( \ell \) is itself a low value and may therefore be safely shared with untrusted code.

Given this specification for readonly, let us now consider a client of readonly that wishes to maintain an invariant on its private (i.e., high-integrity) state:

\[
\text{usetwo } \triangleq \ \text{let } r = \text{ref } 2 \ \text{in} \\
\hspace{1cm} \text{let } w = \text{readonly } r \ \text{in} \\
\hspace{1cm} \text{let } use = \lambda. \text{assert } ((!r) = 2) \ \text{in} \\
\hspace{1cm} (use, w)
\]

Here, the expression usetwo allocates a reference cell \( r \) containing the value 2, and returns a pair of functions, one of which simply asserts that \( r \) continues to contain 2, and the other of which is the result of readonly\( r \). The reference cell \( r \) is, however, kept private (i.e., hidden in the environments of the closures use and w).

Our aim is to verify that usetwo can be safely linked with arbitrary untrusted code. To do this, we first prove that it satisfies the spec \( \{ \top \} \text{usetwo } \{ x. \text{lowval } x \} \) which means that we can always run usetwo and, if we do, it returns a low value. It is easy to see intuitively why this spec holds: reference cell \( r \) always contains 2, which is trivially low, so together with the spec for readonly, this is sufficient to ensure that the closures returned by usetwo are low as well.

Next, we appeal to a general meta-theorem—and one of the main technical results of this paper—called robust safety. Robust safety states that, if some user code satisfies a spec like the one given above for usetwo—i.e., a spec whose postcondition stipulates that the resulting value is low-integrity—then we can run that verified user code under an arbitrary adversarial context \( C \) (i.e., any context \( C \) that does not itself contain any assert statements), and we will be assured that the execution of the resulting program will never result in a violation of any of the user code’s internal assertions. Thus, in the particular case of usetwo, we know that the assertion that \( r \) equals 2 will never fail.

\[2\] The Coq formalization is available online [OCPL 2017].
Robust safety is a well-known meta-theorem in the security literature [Bengtson et al. 2011; Gordon and Jeffrey 2001], but it has not heretofore been employed in the context of object capability programming. One of the central contributions of this paper is the observation that robust safety is exactly the property a language must satisfy in order to support OCPs. Moreover, as we will demonstrate via a range of interesting examples, the notion of low-integrity values is essential to compositionally specifying an OCP’s contribution toward the robust safety of programs that use it.

The remainder of the paper is structured as follows. First, in §2, we introduce some basics of OCPL, along with our formalization of low values, explain how we verify our motivating readonly example, and state the key metatheorems of adequacy and robust safety. In §§3–5, we present specifications for several more complex and realistic OCPs, along with examples of how to use those specifications to verify representative clients. In §6, we discuss related work. Finally, in §7, we conclude with a discussion of future work.

2 ROBUST SAFETY AND OCPL

In this section, we define the semantics of the programming language we will be reasoning about (§2.1), present the main ideas of OCPL and show how to use it to reason formally about our motivating example (§2.2), and state key metatheorems for OCPL (§2.3).

2.1 A Higher-Order Concurrent Heap Language with Assertions

The programming language we consider in this paper, which we call HLA, is a fairly standard higher-order concurrent imperative language, essentially the same as the one studied by Krebbers et al. [2017a], but with one important extension. We define the language in Fig. 1. The core of the language is a call-by-value λ-calculus with recursive functions, products, sums, references, and fork-based concurrency.1 The definitions of free and bound variables and capture-avoiding substitution are standard and omitted. We endow the language with an operational semantics in the style of Felleisen and Hieb [1992]. The head reduction judgment $e; \sigma \rightarrow e'; \sigma'$ describes the single steps of computation that may be taken by individual threads. It means that, starting in state $\sigma$, a thread running expression $e$ may step to expression $e'$ while changing the state to $\sigma'$ and forking off a list of threads running expressions $e'$. Threadpool reduction $T; \sigma \rightarrow T'; \sigma'$ lifts head reduction to lists of concurrently running threads. We leave implicit the choice of operators $unop$ and $binop$, but note that they reduce according to (partial) evaluation functions and are subject to a semantic constraint; for example, the reduction rule for unary operators

$$unop v; \sigma \rightarrow v'; \sigma; \epsilon \quad \text{if eval } unop v = v'$$

employs a partial function eval : $Unop \rightarrow Val \rightarrow Val$ (which, for the robust safety theorem presented below, is assumed to send low-integrity values to low-integrity values). As is standard in semantics for languages with mutable references, locations $\ell$ are not part of the “surface” syntax of the language; they may only arise dynamically during execution. Using compare-and-swap (CAS), one can implement locks (and other concurrency primitives).4 We use the symbol `_` in place of a bound variable to indicate any variable not occurring free in the scope of the binder. In addition to

---

1OCPs are typically studied in the context of an event-driven programming model. We work in the setting of fork-based concurrency because Iris supports it natively and it does not seem to significantly affect reasoning about OCPs.

2The expression $\text{CAS } \ell v_1 v_2$ atomically compares the contents of location $\ell$ to value $v_1$ and, if equal, writes $v_2$ to $\ell$ and returns true; otherwise, it returns false. For simplicity, we do not restrict CAS to comparing first-order, “word-sized” values. This is unrealistic, but we use CAS in only realistic ways. (Spinlocks, in particular, are compatible with such a restriction and suffice for our purposes.)
We define C-style assertions—which we call assumption expressions; the one new feature in HLA, not present in Krebbers et al.’s calculus, is assertion expressions, assert e, which serve to specify safety properties that should always hold dynamically. Assertions in HLA operate a little differently from assertions in languages like C or Java, where failed assertions abort execution or raise an exception. Here, e is a boolean expression. If e evaluates to true, then assert e has no effect. But if e evaluates to false, then assert e has the effect of irreversibly setting

\[\text{Robust and Compositional Verification of Object Capability Patterns}\]

standard derived forms (e.g., n-ary products and let expressions), we write

\[\lambda x. e \triangleq \text{rec } x. e\]
\[\lambda x_1 \cdots x_n. e \triangleq \lambda x_1. \cdots. \lambda x_n. e\]
\[\text{rec } f x_1 \cdots x_n. e \triangleq \text{rec } f x_1. \lambda x_2 \cdots x_n. e\]

and we use pattern-matching notation to deconstruct products, rather than a series of fst and snd projections.

\[\text{Fig. 1. Heap language with assertions}\]

We define C-style assertions—which we call assumption expressions—in §3.
a “goodness bit” $g$, which is maintained as part of the machine state, to $\text{Fail}$. (The bit is initially set to $0\text{K}$.) This goodness bit simply checks whether any assertion expression has dynamically failed during execution. Ultimately, our robust safety theorem will use this goodness bit to ensure that, for properly verified code, the goodness bit will remain $0\text{K}$ throughout execution (and hence all dynamic assert checks must succeed).

The reader may wonder why we employ a goodness bit instead of just saying that assert false gets stuck or aborts the program. The reason is simple: we wish to use OCPL to reason not only about fully verified code but also about the behavior of verified code when linked with untrusted code (that does not itself contain assertions). So it is important that we have a way of verifying Hoare triples even for code that may very well get stuck (i.e., fail to make progress) thanks to dynamic type errors introduced by the untrusted code. We nevertheless want to say that assert expressions in such code always succeed, so we must differentiate assert false from other stuck states.\footnote{Instrumenting the state with a goodness bit is not strictly necessary; for example, one could alternatively use a special machine configuration to indicate failed assertions.}

2.2 A Program Logic for Reasoning about OCPs

We now present some of the essential features of OCPL, our logic for reasoning about OCPs.

Progressive vs. non-progressive triples. OCPL is a Hoare-style program logic derived from Iris, a modern separation logic for higher-order concurrent imperative programs.\footnote{Readers unfamiliar with separation logic can, to a first approximation, read separating conjunction $P \cdot Q$ as conjunction $P \land Q$ and magic wand $P \Rightarrow Q$ as implication $P \Rightarrow Q$.} As such, one of the main assertions in OCPL is the Hoare triple, which is used to specify the behavior of expressions in terms of preconditions and postconditions. The Hoare triple $\{ P \} e \{ x. Q \}_p$ asserts that, assuming $e$ is executed starting in a state satisfying the precondition $P$, then it will execute without any dynamically failing assert expressions, and if it terminates with value $v$, then the final state will satisfy the postcondition $Q$ (which may mention the bound variable $x$). The progress bit $p \in \{ \text{progress}, \text{noprog} \}$ indicates whether the triple is progressive (i.e., ensures that $e$ does not get stuck) or non-progressive.\footnote{Note: this is a point of difference from the original Iris, which only supported progressive triples.} As shorthand, we will write $\{ P \} e \{ x. Q \}$ and $\{ P \} e \{ x. Q \}$, for progressive and non-progressive triples, respectively; the former assertion implies the latter. We often write the postcondition of a Hoare triple as $\{ x_1 \cdot \ldots \cdot x_n. \text{ret} \ pat. Q \}$, which binds the $x_i$ and specifies that any returned value will be precisely $\text{pat}$. This notation is (roughly) syntactic sugar for the post-condition $\{ x. \exists x_1, \ldots, x_n. x = \text{pat} \cdot Q \}$.

Hoare triples in Iris (and thus OCPL) enjoy the standard structural rules for higher-order concurrent separation logic (e.g., the rule of consequence, the frame rule, and monadic bind and return) as well as rules for defining and enforcing logical protocols on physical and ghost state. Readers interested in these aspects of OCPL should consult Jung et al. [2015] for a high-level overview and Jung et al. [2017] for a recent account of Iris’s foundations.

In addition, OCPL enjoys a full set of basic rules for HLA, comprising progressive triples for reasoning about head reductions and non-progressive triples for reasoning about stuck expressions. The following three rules, for example, concern application.

\[
\text{App} \\
\frac{(\text{rec } f \ x \ e) \ \text{closed}}{\{ P \} e[v/x, \text{rec } f \ x \ e/f] \ \{ x. Q \}} \quad \text{AppNRec} \\
\frac{\neg(\exists f \ x \ e) \ u = \text{rec } f \ x \ e}{\{ \top \} \ u u' \ { x. Q }?} \quad \text{AppOpen} \\
\frac{(\text{rec } f \ x \ e) \ \text{closed}}{\{ \top \} (\text{rec } f \ x \ e) u \ { x. Q }?}
\]

\footnote{Readers unfamiliar with separation logic can, to a first approximation, read separating conjunction $P \cdot Q$ as conjunction $P \land Q$ and magic wand $P \Rightarrow Q$ as implication $P \Rightarrow Q$.}
PointstoExclusive
\[ \ell \leftarrow v \star \ell \leftarrow w \vdash \bot \]

HighNotLow
\[ \ell \leftarrow v \star \text{lowloc} \ell \vdash \bot \]

Alloc
\[ \{ \top \} \text{ref } v \{ \ell, \text{ret } \ell. \ell \leftarrow v \} \]

AllocLow
\[ \{ \text{lowval } v \} \text{ref } v \{ \ell, \text{ret } \ell. \text{lowloc } \ell \} \]

Load
\[ \{ \ell \leftarrow v \} ! \ell \{ \text{ret } v. \ell \leftarrow v \} \]

LoadLow
\[ \{ \text{lowloc } \ell \} ! \ell \{ x. \text{lowval } x \} \]

Store
\[ \{ \ell \leftarrow v \} \ell \leftarrow w \{ \text{ret } () . \ell \leftarrow w \} \]

StoreLow
\[ \{ \text{lowloc } \ell \star \text{lowval } v \} \ell \leftarrow v \{ \text{ret } () . \top \} \]

(a) High locations

(b) Low locations

Fig. 2. Selected proof rules for locations

Rule \textit{App} says that, to prove a triple for a closed function application, it suffices to show an analogous triple after \( \beta \)-reduction. Rules \textit{AppNrec} and \textit{AppOpen} give non-progressive triples to applications that, according to the operational semantics of HLA, always get stuck: as such applications never produce a value, they can be given an \textit{arbitrary} postcondition \( Q \).

We omit analogous rules for other expressions that ignore the ambient machine state, turning now to the more interesting rules for assertions and locations.

\textbf{Assertion expressions.} OCPL supports the following rule for assertion expressions.

\textbf{Assert}
\[ \{ P \} e \{ x. x = \text{true } \star Q \}_p \vdash \{ P \} \text{assert } e \{ \text{ret } () . Q \}_p \]

\textbf{Assert} enables reasoning about successful assertions. It says that, to prove a Hoare triple for \textbf{assert } e with postcondition \( Q \) and return value () , it suffices to prove that \( e \) evaluates to \textbf{true} with postcondition \( Q \).

\textbf{High vs. low locations.} OCPL divides memory locations (\textit{i.e.}, mutable references) into two types: \textit{high-integrity} and \textit{low-integrity} (or just \textit{high} and \textit{low} for short). High locations are locations that are private to user code, on which it may place invariants of its choosing, and to which untrusted code should not be given direct, unfettered access. Low locations are locations that may be freely shared with—and may in fact have been allocated by—untrusted code. Note that there is no distinction between high and low locations in the operational semantics of HLA; rather, this distinction is merely something we track in OCPL in order to formally specify the interface between user code and untrusted code.

\textbf{Reasoning about high locations.} Since high locations are locations controlled privately by verified user code, OCPL supports reasoning about them in essentially the same way as one reasons about pointers in traditional separation logic—via the classic “points-to” assertion \( \ell \leftarrow v \). This points-to assertion denotes the knowledge that location \( \ell \) currently points to value \( v \) as well as ownership of \( \ell \). What this means is that if we own \( \ell \), then no other party (\textit{e.g.}, neither another thread nor the current thread’s context) can be simultaneously making any assertion about \( \ell \), so we should have permission to freely read from and write to \( \ell \) without worrying about violating any other party’s reasoning. This reasoning is formalized with standard rules about high locations displayed in Fig. 2a.

\textbf{Reasoning about low locations.} We represent the knowledge that a location \( \ell \) is low via the assertion lowloc \( \ell \). In contrast to the points-to assertion for high locations, the assertion lowloc \( \ell \)
does not denote any ownership of \( \ell \) because as soon as a location is considered safe to be shared with untrusted code, there is no way of knowing what that code will do with it. Rather, lowloc \( \ell \) merely tells us that \( \ell \) is low now and will remain low forever. Moreover, if \( \ell \) is low—and hence safely shareable with untrusted code—then we know that the value \( v \) it points to must also be safely shareable with untrusted code—i.e., \( v \) is a low value.

Of course, this begs the question: what is a low value? Intuitively, a low value is a value from which there is no way to extract a high location. We will make this more precise in a moment. For now, assume we have a predicate \( \text{lowval } v \), which says that \( v \) is a low value.

The description of low locations given above is formalized in the proof rules of Fig. 2b. Rule \text{HighNotLow} says that a location cannot be high and low at the same time. Rules \text{AllocLow}, \text{LoadLow}, and \text{StoreLow} mimic the corresponding rules for allocation, reading, and writing of high locations, except that for low locations, we do not track the precise contents of the location \( \ell \)—we merely insist that \( \ell \) always points to a low value.

\textbf{Lifting low locations to low values.} We return now to the question of what it means for a value \( v \) to be low. Intuitively, a low value is one from which the language constructs of HLA provide no way to get direct access to any high location. This is fundamentally an \textit{extensional} property, i.e., a property about the observations that a program can make (i.e., the information it can extract) when passed the value \( v \). As such, for those readers familiar with classic techniques from program semantics, it will not come as a surprise that a natural way of formally accounting for this property is via a \textit{logical relation}.

Fig. 3 shows the definition of this logical relation, presented in a somewhat more general form, \( \text{lift } \Psi v \). Essentially, \( \text{lift } \Psi v \) is a predicate on values, with the property that \( \text{lift } \Psi v \) is true if \( \Psi \) holds for any location that can be extracted from \( v \). Given this definition, \( \text{lowval } v \) can be defined simply as \( \text{lift lowloc } v \)—i.e., a value is low if any location that can be extracted from it is low.

On literals and unit, \( \text{lift } \Psi \) is trivially true since no location can be extracted from them; on locations, \( \text{lift } \Psi \) is simply \( \Psi \); and on products and sums, \( \text{lift } \Psi \) is defined in the obvious recursive manner. The only interesting case is the one for functions. For a function value \( f \), we want to say that \( \text{lift } \Psi f \) if, whenever we apply \( f \), the resulting term only ever produces values that satisfy \( \text{lift } \Psi \). (This property on applications of \( f \) is expressed via a \textit{non-progressive} Hoare triple since \( f \) may be applied to arguments constructed by untrusted code.) But what arguments should we consider when applying \( f \)? This is where the logical relation comes in: we need only consider argument
values that themselves satisfy $\text{lift } \Psi$, because ultimately we will make sure that all values passed to untrusted code satisfy $\text{lift } \Psi$.

Note that the definition of $\text{lift } \Psi$ in the function case is rather circular, since it quantifies over values that satisfy $\text{lift } \Psi$, because ultimately we will make sure that all values passed to untrusted code satisfy $\text{lift } \Psi$.

To ensure that this definition is well-founded, we rely on OCPL’s support for guarded recursive definitions (inherited from Iris). In OCPL, a definition may be arbitrarily recursive so long as any recursive references are guarded by an occurrence of the $\triangleright$ (“later”) modality. Under the hood, all assertions in OCPL are implicitly indexed by steps of computation—i.e., the model of OCPL is a kind of step-indexed model [Birkedal et al. 2011]—and $\triangleright P$ means that $P$ holds, roughly speaking, “after one step of computation”. Since the fine points of the “later” modality are not particularly relevant to our main contribution, and our use of “later” is standard, we refer the reader to prior work for a more detailed presentation [Appel et al. 2007].

Using the aforementioned structural and basic rules, we can readily derive rules for working with lifted values. For example, the derived rule

$$\text{LiftApp}$$

$\{\text{lift } \Psi v \star \text{lift } \Psi v'\} \triangleright \{x. \text{lift } \Psi x\}$

says that one can always apply a lifted value to a lifted argument, and such applications either get stuck (the rule uses a non-progressive triple) or produce a lifted result. These derived rules help, for instance, in verifying clients of the public membrane (§5), which we specify using $\text{lift }$.

To make concrete this rather abstract tour of OCPL, we return to our motivating example. To verify that $\text{readonly}$ satisfies its specification, we have to show that the function it returns, $\lambda_. ! \ell$, is a low value given a triple $\{\top\} ! \ell \{x. \text{lowval } x\}$ for dereferencing $\ell$. This follows easily by $\text{LiftRec}$. To verify that the expression $\text{usetwo}$ returns a low value, we proceed as follows. From the allocation $\text{ref } 2$ we obtain $\ell \leftrightarrow 2$ for some location $\ell$ (by $\text{Alloc}$). Since we own $\ell$, we are free to transfer ownership of $\ell$ into a shared invariant, which in Iris (and OCPL) is written $\ell \leftrightarrow 2$, stipulating that $\ell$ will always contain 2. (Invariants like $\ell \leftrightarrow 2$, which are established “dynamically” in the course of a program proof and hold persistently thereafter, are a feature inherited directly from Iris [Jung et al. 2015]. We omit rules for working with them here since they are orthogonal to the focus of this paper.) By $\text{Load}$, we easily obtain a lemma

$$\ell \leftrightarrow 2 \vdash \{\top\} ! \ell \{\text{ret } 2. \top\} \quad \text{(†)}$$

stating that, under our invariant, dereferencing $\ell$ always returns 2. To prove that the value $w$ returned by $\text{readonly} \ell$ is low-integrity, we apply $\text{readonly}$’s specification and have to show that dereferencing $\ell$ returns a low value (which is trivial, by (†) and $\text{LiftLit}$). To prove that the function $\text{use } \triangleq \lambda_. \text{assert } ((! \ell) = 2)$ is low-integrity, we apply $\text{LiftRec}$. In this subproof, we have to prove that, under our invariant, the assertion returns a low value (trivial by $\text{Assert}$, (†), $\text{LiftUnit}$). It remains to show that the pair $(w, \text{use})$ is low-integrity given knowledge that both $w$ and $\text{use}$ are low-integrity, which is trivial by $\text{LiftPair}$.

### 2.3 Metatheory

OCPL inherits from Iris the basic metatheorem of adequacy for progressive triples (omitted here), which asserts that expressions verified with progressive triples make progress (i.e., do not get stuck) and that, if such expressions terminate, the postconditions of their triples actually hold. OCPL also enjoys an analogous metatheorem for non-progressive triples, which simply drops the progress guarantee. More interestingly, OCPL enjoys the following metatheorems concerning dynamically checked safety properties. The entire metatheory has been verified formally in Coq [OCPL 2017].
Theorem \textsc{AdeqacySafety}. If an expression is verified and run in a good state, we can observe that every reachable state is good (\emph{i.e.}, no assertions fail):

\[
\{ \top \} \ e \ \{ \top \}_p \ (e); (h, \OK) \rightarrow^* T'; (h', g')
\]

\[
g' = \OK
\]

Theorem \textsc{RobustSafety}. Let $\text{AdvCtx}$ denote the set of HLA contexts containing neither locations nor assertions. If expression $e$ is closed and has been verified to return only low values, then for every adversarial context $C$, on running $C[e]$ from an initial state, we can observe that every reachable state is good (\emph{i.e.}, no assertions fail):

\[
C \in \text{AdvCtx} \quad e \ \text{closed} \quad \{ \top \} \ e \ \{ \text{lowval} \}_p \quad (C[e]); (\emptyset, \OK) \rightarrow^* T'; (h', g')
\]

\[
g' = \OK
\]

Robust safety captures our informal distinction between “user code” and “untrusted code”. Both are written in HLA, but user code must be verified in OCPL and may contain assertion statements, whereas untrusted code need not be verified and is not permitted to contain assertion statements. Untrusted code may also not contain references to memory locations $\ell$, since those are not part of the surface syntax of the language. The theorem says that verified user code can be linked with untrusted code, while remaining safe (\emph{i.e.}, its internal assertion statements will never assert false).

3 DYNAMIC SEALING

We now consider one of the oldest and most influential OCPs: \textit{dynamic sealing}, also called the sealer-unsealer pattern. Originally proposed by \textcite{morris}, dynamic sealing makes it possible to support data abstraction in the absence of static typing. In this section, we show how OCPL supports compositional reasoning about dynamic sealing. In particular, we show how to implement dynamic sealing in HLA and how to give a compositional specification for this implementation, from which we derive useful specifications for interesting abstractions built on top of it and prove robust safety for representative clients. (We consider an alternative implementation of the OCP, satisfying a slightly weaker specification, in Appendix A. We also show how ideal specifications for cryptographic signing and encryption primitives can be derived from the specification of dynamic sealing in Appendix B.)

The functionality of dynamic sealing. \textcite{morris} introduced dynamic sealing to enforce data abstraction while interoperating with untrusted, potentially ill-typed code. He stipulated a function $\text{make\_seal}$ for generating pairs of functions ($\text{seal}, \text{unseal}$), such that (i) for every value $v$, $\text{seal\_}v$ returns a value $v'$ serving as an opaque, low-integrity proxy for $v$; and (ii) for every value $v'$, $\text{unseal\_}v'$ returns $v$, if $v'$ was produced by $\text{seal\_}v$, and otherwise gets stuck. The key point is that this $\text{seal\_unseal}$ pair supports data abstraction: the client of these functions can freely pass sealed values to untrusted code since they are low-integrity, while at the same time imposing whatever internal invariant it wants on the underlying values that they represent.

To see how this is useful, consider a simple client of dynamic sealing, namely Morris’s example of a library for integer intervals (Fig. 4). Let $[n_1, n_2]$ denote the set $\{n_1, n_1 + 1, \ldots, n_2 - 1, n_2\}$. The function $\text{intervals}$ returns several interval-manipulating routines: $\text{make\_int} n_1 n_2$ constructs $[\min n_1 n_2, \max n_1 n_2]$, $\text{imin} [n_1, n_2]$ returns $n_1$, $\text{imax} [n_1, n_2]$ returns $n_2$, and $\text{isum} [n_1, n_2] [n_1', n_2']$ returns $[n_1 + n_1', n_2 + n_2']$.

These routines use dynamic sealing to enforce the internal data representation of intervals, namely that the interval $[n_1, n_2]$ is represented by the pair $(n_1, n_2)$, which is critical to ensuring correctness of the library. In particular, notice that $\text{seal}$ and $\text{unseal}$ are kept private to the $\text{intervals}$ implementation, which means it can enforce that the only values sealed with $\text{seal}$ are pairs $(n_1, n_2)$.
representing intervals (i.e., where \( n_1 \leq n_2 \)). Consequently, the \( \text{imin} \) (resp. \( \text{imax} \)) function can simply return the first (resp. second) component of its argument after unsealing it, because it \textit{knows} that, even if the argument comes from untrusted code, \textit{so long as the unsealing succeeds}, the resulting value will be a pair where the first (resp. second) component represents the lower (resp. upper) bound of the input interval. Furthermore, a client of \( \text{intervals} \) knows that it applies both \( \text{imin} \) and \( \text{imax} \) to an arbitrary untrusted value \( v \), and both operations succeed, producing values \( v_1 \) and \( v_2 \), then \( v \) must indeed represent a proper interval \([n_1,n_2]\) (with \( n_1 \leq n_2 \)), and the resulting values of \( \text{imin} \) and \( \text{imax} \) are precisely \( v \)'s lower and upper bounds (i.e., with \( v_1 = n_1 \) and \( v_2 = n_2 \)). In this way, dynamic sealing affords programmers the essential functionality of data abstraction, even when interfacing with untrusted code, at the cost of some simple dynamic checks at the boundaries of the abstraction.

\textit{Implementation of dynamic sealing.} We implement dynamic sealing in HLA as follows.\(^9\)

\[
\text{make} = \lambda_. \text{let} \ (\text{seal}, \text{unseal}) = \text{make} () \text{ in } \\
\text{let} \ \text{makeint} = \lambda n_1, n_2. \ \text{seal}\ (\text{if} \ n_1 \leq n_2 \ \text{then} \ (n_1, n_2) \ \text{else} \ (n_2, n_1)) \ \text{in } \\
\text{let} \ \text{imin} = \lambda i. \ \text{fst} \ (\text{unseal} i) \ \text{in } \\
\text{let} \ \text{imax} = \lambda i. \ \text{snd} \ (\text{unseal} i) \ \text{in } \\
\text{let} \ \text{isum} = \lambda i. \ \text{let} \ x = \ \text{unseal} i \ \text{in} \ \lambda j. \ \text{let} \ y = \ \text{unseal} j \ \text{in } \\
\text{seal} \ (\text{fst} \ x + \text{fst} \ y, \ \text{snd} \ x + \text{snd} \ y) \\
\text{in} \ (\text{makeint}, \ \text{imin}, \ \text{imax}, \ \text{isum})
\]

Fig. 4. Library for integer intervals

The function \( \text{make} \) allocates a fresh lookup table \( \text{tbl} \), which is used to store the mapping between sealed values and their proxies, and access to which is shared by the \( \text{seal} \) and \( \text{unseal} \) functions that \( \text{make} \) returns. To ensure proper synchronization between table accesses during calls to \( \text{seal} \) and \( \text{unseal} \), \( \text{make} \) also creates a lock via the call to \( \text{makesync} \). (The latter returns a higher-order function \( \text{sync} \), which ensures mutual exclusion among any expressions \( e_i \) run under \( \text{sync} \ (\lambda_. \ e_i) \). For more details on \( \text{makesync} \), see Appendix F.) An entry \([k \mapsto v] \) in \( \text{tbl} \) signifies that location \( k \) is a low-integrity proxy for sealed value \( v \). To seal a value \( v \), we allocate a fresh, low location \( k \), extend the table, and return \( k \). To unseal a value \( v' \), we require that \( v' \) be a location \( k \) and then look up \( k \) in the table.

To test whether the argument to \( \text{unseal} \) is a location, we use a primitive unary operator \( \text{isloc} \) (with boolean return type), as well as an \textit{assumption expression}. The expression \( \text{assume} e \) resembles a C- or Java-style assertion: it returns \text{true} if \( e \) evaluates to \text{true}; otherwise, it gets stuck. It is easy

\(^9\)We discuss the straightforward functions \( \text{makesync} \), \( \text{mapempty} \), \( \text{mapinsertnew} \), and \( \text{maplookup} \) in Appendix F. Note that \( \text{maplookup} f k \) gets stuck if location \( k \) is not in the domain of the partial function represented by value \( f \).
Data abstraction.

\[
\text{MakeSealSpec} \quad \{ \top \} \quad \text{make} = \{ v_1, v_2, r, \text{ret} \} \quad \text{is} \quad \text{seal} \quad v_1, \phi \star \text{is unseal} \quad v_2, \phi
\]

\[
\text{SealSpec} \quad \{ \text{is} \quad \text{seal} \quad v, s \star \phi \star v \} \quad s \quad v \quad \{ x \} \quad \text{is} \quad \text{sealed} \quad v \quad x \star \phi
\]

\[
\text{UnsealSpec} \quad \{ \text{is} \quad \text{unseal} \quad v, u \star \phi \star v \} \quad u \quad v \quad \{ \text{ret} \} \quad \top
\]

\[
\text{UnsealAnySpec} \quad \{ \text{is} \quad \text{unseal} \quad v, u \star \phi \star v \} \quad u \quad v \quad \{ \text{x} \} \quad \text{is} \quad \text{sealed} \quad v \quad x \star \phi
\]

\[
\text{SealedInv} \quad \text{is} \quad \text{sealed} \quad v \quad u \star \phi \star v \quad \text{−} \star \phi
\]

\[
\text{SealedAgree} \quad \text{is} \quad \text{sealed} \quad v \quad u \star \phi \star v \quad \text{−} \star \phi
\]

Low values.

\[
\text{SealedLow} \quad (\forall u) \quad \text{lowval} \quad u \quad \vdash \phi \quad u
\]

\[
\text{UnsealedLow} \quad (\forall u) \quad \phi \quad v \quad \vdash \text{lowval} \quad u
\]

Fig. 5. Sealing interface (presupposing \( \phi \) persistent)

to define assumption expressions using a stuck term \( \text{abortion} \):

\[
\text{abortion} \triangleq 0 \quad 0
\]

\[
\text{assume} \ e \triangleq \text{if} \ e \text{then} () \text{else} \text{abortion}
\]

These satisfy the following specifications.

\[
\text{Abort} \quad \{ \top \} \quad \text{abortion} \quad \{ x, \text{Q} \}
\]

\[
\text{Assume} \quad \{ P \} \quad e \quad \{ x \} \quad x = \text{true} \text{→} \text{Q} \quad \vdash \{ P \} \quad \text{assume} \quad e \quad \{ \text{ret} () \}, \text{Q}
\]

\( \text{Abort} \) follows trivially from \( \text{AppNrec} \) and gives \( \text{abortion} \) a non-progressive triple because in fact \( \text{abortion} \) always gets stuck and never produces a value; correspondingly, it can also be given an arbitrary postcondition \( \text{Q} \). Compared to \( \text{Assume} \) in §2.2, \( \text{Assume} \) (i) uses non-progressive triples since \( \text{assume} \ e \) may get stuck, and (ii) only requires the postcondition \( \text{Q} \) to be shown to hold under the \text{assumption} that \( e \) returns true.

Specifying dynamic sealing. The motivation for dynamic sealing given above was completely informal. Let us now see how OCPPL lets us formalize it.

We specify dynamic sealing in Fig. 5. Rule \( \text{MakeSealSpec} \) for allocating a sealer-unsealer pair ties the two functions it returns to an abstract (logical) name \( \gamma \) and representation invariant \( \phi \). In particular, the assertions\(^1\) \( \text{is} \quad \text{seal} \quad v_1, \phi \) and \( \text{is} \quad \text{unseal} \quad v_2, \phi \) represent knowledge that \( v_1 \) and \( v_2 \) are the seal and unseal functions associated with the sealer-unsealer pair named \( \gamma \) with representation invariant \( \phi \). Similarly, the assertion \( \text{is} \quad \text{sealed} \quad v, u \star \phi \star v \) represents knowledge that \( v \) is a low-integrity proxy for value \( v \) (for the sealer-unsealer pair named \( \gamma \) with representation invariant \( \phi \)). This relation is functional in \( v \) —i.e., unsealing the same \( v \) twice will produce the same \( v \) (\( \text{SealedAgree} \))—and implies \( \phi \) \( v \) —i.e., that the unsealed value \( v \) must satisfy the representation invariant (\( \text{SealedInv} \)). Conversely, to seal a value \( v \), one is required to prove \( \phi \) \( v \) (\( \text{SealLow} \)). The progressive triple \( \text{UnsealedLow} \) is suitable for use when one already knows that \( v \) and \( v' \) are related; it returns \( v \). The non-progressive triple \( \text{UnsealedAnySpec} \) returns the value \( v \) related to \( v' \), or gets stuck.

\(^1\)In our specifications, predicates whose names start with “is” produce, when fully applied, persistent propositions (and are themselves called persistent predicates). Persistent propositions may be regarded as intuitionistic (technically, they may be freely duplicated). A sealer-unsealer pair’s representation invariant \( \phi \) must be persistent.
Properties.

\[
\text{MinSpec} \quad \{ \text{ismin } \gamma \text{ imin } \ast \text{isinterval } \gamma n_1 n_2 i \} \text{ imin } i \{ \text{ret } n_1. \ \top \}
\]

\[
\text{IntervalInv} \quad \text{isinterval } \gamma n_1 n_2 i \vdash n_1 \leq n_2
\]

\[
\text{IntervalAgree} \quad \text{isinterval } \gamma n_1 n_2 i \ast \text{isinterval } \gamma n'_1 n'_2 i \vdash n_1 = n'_1 \ast n_2 = n'_2
\]

Non-progressive triples.

\[
\text{MinAnySpec} \quad \{ \text{ismin } \gamma \text{ imin } \} \text{ imin } v \{ n_1 n_2, \text{ret } n_1. \text{isinterval } \gamma n_1 n_2 v \}?
\]

\[
\text{MaxAnySpec} \quad \{ \text{ismax } \gamma \text{ imax } \} \text{ imax } v \{ n_1 n_2, \text{ret } n_2. \text{isinterval } \gamma n_1 n_2 v \}?
\]

Low values.

\[
\text{IntervalLow} \quad \text{isinterval } \gamma n_1 n_2 i \vdash \text{lowval } i
\]

\[
\text{MinLow} \quad \text{ismin } \gamma \text{ imin } \vdash \text{lowval } \text{imin}
\]

\[
\text{MaxLow} \quad \text{ismax } \gamma \text{ imax } \vdash \text{lowval } \text{imax}
\]

Fig. 6. Intervals interface (selected rules—see Appendix C)

Finally, the three rules at the bottom of Fig. 5 concern the lowval relation. Rule \text{SealedLow} says that all sealed values are low values—indeed, the whole point of using sealing is to produce low-integrity proxy values—while rules \text{SealLow} and \text{UnsealLow} say when the seal and unseal functions themselves can be considered low values. Intuitively, seal and unseal can be considered low values whenever doing so does not either (i) violate the representation invariant \(\phi\) or (ii) result in high-integrity values flowing to a low context. Thus, seal is low so long as any value that is passed to it (i.e., any low value) satisfies \(\phi\), and unseal is low so long as any value returned by it (i.e., any value that satisfies \(\phi\)) is low. (We show how to gainfully employ low seal and unseal functions in Appendix B.)

The specification for dynamic sealing from Fig. 5 can be straightforwardly used to derive an analogous specification for the interval-manipulation routines generated by \text{intervals}, as we described above. In particular, by choosing the representation invariant \(\phi v \equiv \exists n_1, n_2. v = (n_1, n_2) \ast n_1 \leq n_2\), we can easily verify the rules shown in Fig. 6 (the full specification for \text{intervals} is given in Appendix C). The assertion isinterval \(\gamma n_1 n_2 i\) represents knowledge that value \(i\) represents interval \([n_1, n_2]\) in the instance of the intervals library with abstract name \(\gamma\). A value may represent at most one interval (\text{IntervalAgree}). A set of progressive triples (e.g., \text{MinSpec}) account for our informal specification and are suited to reasoning about values known to represent intervals. A set of non-progressive triples are suited to reasoning about values that might represent intervals. Rule \text{MinAnySpec}, for example, says that for any value \(v\), \text{imin } v might get stuck, but if it terminates with value \(\hat{v}\), then \(v\) represents some interval with minimum \(n_1\) and \(\hat{v} = n_1\). Lastly, there are rules (e.g., \text{IntervalLow} and \text{MinLow}) expressing the fact that values representing intervals, and the interval routines themselves, may be safely shared with untrusted code. Crucial to the soundness of these rules is the fact that the seal function used internally by \text{intervals} is not shared with untrusted code (i.e., not low): according to rule \text{SealLow}, in order for seal to be treated as low, the representation invariant \(\phi\) would have to be satisfied by all low values, which it clearly is not.
With the spec for \textit{intervals} in hand, we can readily prove that the following simple but illustrative client of \textit{intervals} is robustly safe.

\begin{verbatim}
client ≜ let cap = intervals () in
  let (makeint, imin, imax, isum) = cap in
  let check = λ j. assert (imin j ≤ imax j) in
  (check, cap)
\end{verbatim}

The expression constructs an instance \textit{cap} of the intervals library, along with a function \textit{check} which takes an arbitrary value \textit{j} as its argument and asserts that \textit{imin j} is no greater than \textit{imax j}. Intuitively, even if \textit{client} is shared with untrusted code, this assertion must always succeed, because if the applications of \textit{imin} and \textit{imax} do not get stuck, it means that \textit{j} is a proper interval value, whose lower bound is \leq its upper bound.

Formally, this is guaranteed as follows. First, using the spec for \textit{intervals}, we can prove \[ \{\top\} \textit{client} \{ x. \text{lowval x} \} \]

The key step in the proof involves showing that the assertion in \textit{check} succeeds for arbitrary \textit{j}, which follows directly from \textit{MinAnySpec}, \textit{MaxAnySpec}, \textit{IntervalAgree}, and \textit{IntervalInv}. Second, we appeal to \textit{Theorem RobustSafety} from §2.3, which implies that the assertion in \textit{check} will not fail, even when \textit{client} is linked with untrusted code.

4 CARETAKER

Next, we consider another well-known OCP, the caretaker pattern [Miller and Shapiro 2003; Miller 2006]. This OCP allows verified (trustworthy) code to grant untrusted code access to a high-integrity resource (a high-integrity location or an API that modifies high-integrity locations), and subsequently disable or enable the access at any time. When the caretaker is enabled, untrusted code can access the resource; when the caretaker is disabled, untrusted code cannot access the resource and the verified code has full control over the resource. The caretaker pattern is useful when the verified code wants to ensure that the untrusted code can access the resource only while some invariant holds. Disabling the caretaker allows the verified code to temporarily break the invariant, secure in the knowledge that untrusted code won’t be able to access the resource until the caretaker is re-enabled.

In this section, we first implement a \textit{caretaker for APIs} in HLA, and specify and verify it in OCPL. Then, we use the API caretaker to implement a second \textit{caretaker for locations} and, again, specify and verify it. Finally, we present a simple client for the location caretaker and establish that it is robustly safe.

\textit{API caretaker}. The API caretaker allows verified code to share revokable access to any set of functions, which may have side-effects.

\begin{verbatim}
makecaretaker ≜ λ _. let enabled = ref false in let sync = makesync() in (sync, enabled)
  wrap ≜ λ (sync, enabled) f x. sync (λ _. assume (! enabled); f x)
  enable ≜ λ (sync, enabled). sync (λ _. enabled ← true)
  disable ≜ λ (sync, enabled). sync (λ _. enabled ← false)
\end{verbatim}

The function \textit{makecaretaker} returns a new caretaker \textit{ct}, which comprises a fresh lock \textit{sync}, whose purpose is described soon, and a fresh boolean reference \textit{enabled}. The caretaker is disabled (enabled) when \textit{enabled} is false (true). The functions \textit{enable ct} and \textit{disable ct} enable and disable the caretaker \textit{ct} by setting \textit{enabled} appropriately. The function \textit{wrap ct f} wraps the function \textit{f} in the caretaker...
Robust and Compositional Verification of Object Capability Patterns

\[
\text{EnabledExclusive}
\]

\[
\text{enabled } \gamma \ b_1 \ \ast \ \text{enabled } \gamma \ b_2 \ \vdash \ \bot
\]

\text{MakeCaretakerSpec}

\{ T \} \ makecaretaker ( ) \ { ct \ \gamma, \ ret. \ iscaretaker \ \gamma \ \text{ct} \ \ast \ \text{enabled } \gamma \ \text{false} } \\
\text{CanWrap}

\text{canwrap } f \ R \ \triangleq \ \forall v. \ \{ \text{lowval } v \ \ast \ R \} \ f \ v \ \{ x' \text{. lowval } x' \ \ast \ R \},

\text{WrapSpec}

\{ \text{iscaretaker } \gamma \ \text{ct} \ \ast \ \text{canwrap } f \ R \} \ \text{wrap } f \ \{ f' \text{. lowval } f' \}

\text{EnableSpec}

\{ \text{iscaretaker } \gamma \ \text{ct} \ \ast \ \text{enabled } \gamma \ \text{false } \ast \ R \} \ \text{enable } ct \ \{ \text{ret } () . \ \text{enabled } \gamma \ \text{true} \}

\text{DisableSpec}

\{ \text{iscaretaker } \gamma \ \text{ct} \ \ast \ \text{enabled } \gamma \ \text{true} \} \ \text{disable } ct \ \{ \text{ret } () . \ \text{enabled } \gamma \ \text{false } \ast \ R \}

Fig. 7. API caretaker interface

c, returning a function that behaves exactly like \( f \) when \( ct \) is enabled, and gets stuck when \( ct \) is disabled. Additionally, accesses to all functions wrapped in \( ct \) are serialized using the lock \( \text{sync} \).

To use this interface, verified code creates a caretaker \( ct \) and holds it privately. It can then wrap any number of API functions using \( \text{wrap} \) and disclose the wrapped functions to untrusted code. The untrusted code’s access to all those functions can be simultaneously disabled and enabled by calling \( \text{disable } ct \) and \( \text{enable } ct \), respectively.

\textit{API caretaker specification.} The goal of using the API caretaker is to ensure that untrusted code can access wrapped functions only while some logical resource or invariant \( R \) holds on the heap. Our specification of the API caretaker in Fig. 7 formalizes this intuition. The assertion \( \text{iscaretaker } \gamma \ \text{ct} \ast R \) represents knowledge that value \( ct \) is a caretaker with (logical) name \( \gamma \) whose wrappers allow (untrusted code) access to wrapped functions only when \( R \) holds. The assertion \( \text{enabled } \gamma \ b \) represents exclusive ownership of the (verified code’s) right to enable and disable all wrappers created using the caretaker named \( \gamma \) as well as knowledge that the caretaker is currently enabled (if \( b = \text{true} \)) or disabled (otherwise).

When applying \( \text{MakeCaretakerSpec} \), one may pick an arbitrary invariant \( R \). The spec returns a disabled caretaker tied to \( R \) and a fresh name \( \gamma \). To enable \( ct \), the (verified) code calling \( \text{enable} \) must establish that \( R \) holds (rule \( \text{EnableSpec} \)). Dually, rule \( \text{DisableSpec} \) says that disabling \( ct \) provides ownership of \( R \) to the caller (verified code).

Rule \( \text{WrapSpec} \) is at the heart of our specification. It says that to wrap a function \( f \) using \( ct \), one has to prove that \( f \), when applied to any low value \( v \) (possibly provided by the untrusted code), \( \text{preserves} \) the invariant \( R \) and returns a low value. We capture this client responsibility in the precondition (\( \text{canwrap } f \ R \) on \( \text{wrap} \)). So, any wrapped function \( f \) can assume \( R \) in its precondition but it must re-establish \( R \) if it terminates (note that the triple for \( f \ v \) in rule \( \text{CanWrap} \) is non-progressive). This ensures that while \( ct \) is enabled, calls to the wrapped functions by the untrusted code preserve \( R \). While \( ct \) is disabled, verified code can change the state to break \( R \) but, prior to re-enabling \( ct \), it must re-establish \( R \).

The implementation of the API caretaker verifies against this specification. We note that the specification and verification of the API caretaker closely resemble similar efforts for specifying and verifying locks in concurrent programs [Dinsdale-Young et al. 2010]. Based on this observation, we
The function \( \text{makelocct} \) below, facilitates revokable and mediated read and write access to a location. Specifically, it ensures that the location is accessed by untrusted code only while some stipulated predicate \( \Psi \) holds on the location’s contents.

\[
\text{makelocct} \equiv \lambda rmon wmon r. \text{let } ct = \text{makecaretaker}() \text{ in} \\
\text{let } read = \text{wrap} ct (\lambda_. \text{rmon} (!r)) \text{ in} \\
\text{let } write = \text{wrap} ct (\lambda x. r \leftarrow (wmon x) \text{ in} \\
(\text{ct, (read, write)})
\]

The function \( \text{makelocct} \), when applied to a function \( f_r \), a function \( f_w \), and a location \( \ell \), returns a pair \( (ct, (\text{read}, \text{write})) \). The API caretaker \( ct \) controls whether or not the functions \( (\text{read, write}) \) are enabled. When \( ct \) is enabled, the function \( \text{read} \) reads \( \ell \) and filters the read value through \( f_r \). Similarly, \( \text{write} \) writes \( \ell \) after filtering the value to be written through \( f_w \). Thus, \( f_r \) and \( f_w \) mediate reads from and writes to \( \ell \). Consider, for example, an application \( \text{write} v \), representing a request to write value \( v \) to location \( \ell \). If \( ct \) is enabled, the application reduces to \( \ell \leftarrow (f_w v) \) and \( f_w \) gets to decide what is written.

To use the location caretaker on a location \( \ell \), verified code invokes \( \text{makelocct} f_r f_w \ell \) with appropriate \( f_r \) and \( f_w \). It holds \( \ell \) and the returned API caretaker \( ct \) private, but passes \( \text{read} \) and \( \text{write} \) to untrusted code. It can then enable and disable access to the protected location using the calls \( \text{enable} ct \) and \( \text{disable} ct \), respectively. While \( ct \) is enabled, all reads and writes to \( \ell \) are mediated by \( f_r \) and \( f_w \), respectively.

**Location caretaker specification.** Our location caretaker specification (Fig. 8) ensures that the value in the protected location \( \ell \) satisfies some stipulated predicate \( \Psi \) whenever the location is accessible to the untrusted code. The proposition \( \text{islocct} \gamma ct \ell \Psi \) means that value \( ct \) is an API caretaker for location \( \ell \) with logical name \( \gamma \) and predicate \( \Psi \) governing the contents of location \( \ell \).
when the caretaker is enabled. Logical names and propositions of the form enabled $y b$ serve the same purpose as in the API caretaker interface.

The triple $\text{MakeLocCtSpec}$ specifies the function $\text{makelocct}$ and imposes conditions on the function’s first two arguments, $f_r$ and $f_w$. Since $f_r$ receives a value read from the protected location, $f_r$’s input can be assumed to satisfy $\Psi$. Since the output of $f_r$ will be returned to untrusted code, that output must be low. Hence, $f_r$ must transform values satisfying $\Psi$ to low values. Dually, since $f_w$ receives a value from untrusted code and its output is written to the protected location, $f_w$ must transform low values to values satisfying $\Psi$. The postcondition for $\text{makelocct}$ says that the returned functions $\text{read}$, $\text{write}$ are low, so they can be passed to untrusted code safely. The precondition of $\text{enable}$ insists that $\ell$ point to a value $v$ satisfying $\Psi$ before the caretaker is enabled (rule $\text{LocCtEnableSpec}$). Dually, the postcondition of $\text{disable}$ reveals the fact that $\ell$ points to a value $v$ satisfying $\Psi$ (rule $\text{LocCtDisableSpec}$).

The location caretaker’s code satisfies this specification, assuming the specification of the API caretaker (Fig. 7). To illustrate how programs may use a location caretaker, and how such programs may be verified, we consider the following very simple program, $\text{client}$.

$$\text{asserteven} \triangleq \lambda n. \text{assert (even n); } n$$
$$\text{assumeeven} \triangleq \lambda n. \text{assume (even n); } n$$

$$\text{client} \triangleq \text{let } r = \text{ref } 0 \text{ in }$$
$$\text{let } (ct, w) = \text{makelocct asserteven assumeeven } r \text{ in }$$
$$\text{enable } ct;$$
$$\text{let } \text{sync} = \text{makesync } \text{in }$$
$$\text{let } \text{use} = \text{sync}(\lambda_. \text{disable ct; assert even (!r); }$$
$$\text{r }\leftarrow 1; \text{r }\leftarrow 0; \text{enable ct})$$

$$\text{in } (\text{use, w})$$

The expression $\text{client}$ constructs a reference cell $r$ (initially containing $0$) and constructs and immediately enables a location caretaker $ct$ serving access to $r$. The goal is to maintain the invariant that untrusted code only sees even numbers in $r$. To ensure this invariant, the location caretaker $ct$ is created with the write filter $f_w = \text{assumeeven}$, which gets stuck unless the value being written is an even number. The read monitor, $f_r = \text{asserteven}$, checks that the value being read from $r$ is indeed even. Additionally, $\text{client}$ exposes to its (untrusted) context a function $\text{use}$ that (within the scope of an exclusive lock, $\text{sync}$) locally disables the caretaker and temporarily breaks the invariant by writing 1 to $r$.

Using the specification of the location caretaker, we prove that $\text{client}$ satisfies the triple

$$\{ \top \} \text{client} \{ x. \text{lowval x} \}$$

By Theorem RobustSafety, $\text{client}$ is robustly safe. This means that irrespective of how the (untrusted) context calls $\text{use}$ and the wrapped read/write interface $\text{w}$, it can never observe a non-even number in $r$ (else, the assertion in $\text{asserteven}$ would fail).

5 MEMBRANE

When verified (trustworthy) and untrusted code interoperate, a general concern is that values passed from verified to untrusted code may accidentally reveal high-integrity locations. The membrane pattern [Miller 2006; Miller et al. 2008; Google, Inc. 2015] was designed to offset this possibility. A membrane is a bidirectional transformation on values passing from verified to untrusted code and vice versa. In the verified-to-untrusted direction, it sanitizes values to make the extraction of
high-integrity locations impossible. A trivial way to implement the membrane is to use the *seal* function of §3, which replaces all values with proxies. However, these proxies cannot be *used* by untrusted code, other than by passing them back to the verified code. To address this shortcoming, the membrane pattern uses a *deep inspection* of values to selectively hide high-integrity locations inside values, while preserving their overall structure (pairs map to pairs, functions map to functions, etc.). This allows the untrusted code to use the transformed values, while still ensuring that it won’t get access to high-integrity locations.

While the specifics of the transformation depend on the language and security objectives of the application, a common core of all membranes is a function that *lifts* a use case-specific bidirectional transformation on locations to a bidirectional transformation on values. We first define this function, *membrane*, in HLA below, show its OCPL specification and verify the function. Then, we use this function to implement a specific membrane that we call the *public membrane*. This membrane replaces each high-integrity location nested in a value with a fresh *shadow* location and provides the verified code special functions to inspect those shadow locations. This is similar to how the membrane pattern is implemented in Google’s Caja, a JavaScript library for securing communication between mutually distrusting domains in web applications [Miller et al. 2008; Google, Inc. 2015].

**Membrane code.** The function *membrane* that forms the common core of the membrane pattern is defined below. This is a higher-order function that takes as its first two arguments two other functions, *locout* and *locin*, both of type *Loc → Val*. The function *locout* defines how locations crossing from verified to untrusted code are transformed by the membrane. Dually, the function *locin* defines how locations crossing in the other direction, from untrusted to verified code, are transformed. Given these two arguments, *membrane locout locin* is a function of type *Val → Val* that transforms values passing from verified to untrusted code. The function for transforming values passing in the other direction—from untrusted to verified code—is obtained by reversing the arguments to *membrane*, i.e., it is *membrane locin locout*.

\[
\textit{membrane} ≜ \text{rec } \textit{memb} \textit{locout} \textit{locin} \textit{x}.
\]

\[
\begin{align*}
\text{let } \textit{wrap} &= \textit{memb} \textit{locout} \textit{locin} \textit{in} \\
\text{if isfun } \textit{x} \text{ then let } \textit{unwrap} &= \textit{memb} \textit{locin} \textit{locout} \textit{in} \\
&\quad \lambda y. \textit{wrap}(\textit{x} (\textit{unwrap} y)) \\
\text{else if isloc } \textit{x} \text{ then } \textit{locout} \textit{x} \\
\text{else if islit } \textit{x} \text{ then } \textit{x} \\
\text{else if } \textit{x} = () \text{ then } () \\
\text{else if ispair } \textit{x} \text{ then } (\textit{wrap} (\textit{fst} \textit{x}), \textit{wrap} (\textit{snd} \textit{x})) \\
\text{else ifinl } \textit{x} \text{ as inl } \textit{x}’ \Rightarrow \textit{inl} (\textit{wrap} \textit{x}’) \\
\text{else ifinr } \textit{x} \text{ as inr } \textit{x}’ \Rightarrow \textit{inr} (\textit{wrap} \textit{x}’) \\
\text{else assert false} \quad // i.e., not reached
\end{align*}
\]

Internally, *membrane* recurses on the structure of the value \(x\) being transformed. When the value is a location, the result is simply \(\textit{locout} \textit{x}\). When the value is a literal, it is returned immediately. When the value is a pair, *membrane* recurses on the two components of the pair. The interesting case arises when the value \(x\) is a function. In this case, *membrane* returns a function, which when applied (by the untrusted code), first recursively applies the membrane to the untrusted argument \(y\).

---

11Google’s Caja partly automates the invocation of the membrane transformation by rewriting untrusted code. The automation is orthogonal to the specification and verification of the membrane pattern itself, so we do not model it here.
then applies the given function \( x \) to the transformed argument, and then re-applies the membrane recursively to the result. Importantly, the membrane is applied in the untrusted-to-verified direction to the function argument \( y \) and in the verified-to-untrusted direction to the result of the function. Technically, the function \( x \) is transformed to \( \text{wrap} \circ x \circ \text{unwrap} \), where \( \text{wrap} \≜ \text{membrane locout locin} \) and \( \text{unwrap} \≜ \text{memb locin locout} \) are recursive instantiations of \( \text{membrane} \) in the verified-to-untrusted and untrusted-to-verified directions, respectively.

**Membrane specification.** Our specification of \( \text{membrane} \) formalizes the intuition that \( \text{membrane} \) lifts transformations on locations to transformations on values. The specification is shown in Fig. 9. The defined predicate \( \text{ismon} p \circ \Psi_1 \circ \Psi_2 \) means that \( \nu \) is a function that transforms values satisfying the predicate \( \Psi_1 \) to values satisfying the predicate \( \Psi_2 \) (the progress bit \( p \) is needed for technical reasons, that readers may ignore). The specification of \( \text{membrane} \) says that if \( \text{locout} \) transforms locations satisfying \( \Psi_1 \) to values satisfying \( \Psi_2 \) and \( \text{locin} \) does the reverse, then \( \text{membrane locout locin} \) transforms values satisfying lift \( \Psi_1 \) to values satisfying lift \( \Psi_2 \), where lift is the predicate transformer defined in Fig. 3. Hence, \( \text{membrane} \) really "lifts" the transformation on locations to a transformation on values in a precise technical sense.

This specification of \( \text{membrane} \) is very general, since it holds for any predicates \( \Psi_1 \) and \( \Psi_2 \). In any use of \( \text{membrane} \), these predicates can be instantiated to match what the arguments \( \text{locout} \) and \( \text{locin} \) do. (Later, we show a specific instantiation with \( \Psi_2 = \text{lowloc} \).)

Despite the specification’s generality, \( \text{membrane} \) is easily verified against it. In the recursive cases, the proof obligations match the inductive hypotheses precisely because of the concordance between the pattern matches in the definitions of lift (Fig. 3) and \( \text{membrane} \).

**Public membrane.** Next, we describe how the function \( \text{membrane} \) can be used to construct a specific membrane, which we call the **public membrane**. This membrane is similar to the membrane used in Google’s Caja library [Miller et al. 2008; Google, Inc. 2015]. The public membrane maintains a unique low-integrity shadow location for every high-integrity location that the verified code declares as important. When values cross from verified to untrusted code, all nested high-integrity locations in them are effectively “replaced” with the corresponding low-integrity shadows (this transformation is implemented using \( \text{membrane} \)). Thus, the untrusted code only sees shadow locations, not the high-integrity locations. Additionally, the public membrane provides the verified code special functions, \( \text{shadowread} \) and \( \text{shadowwrite} \), to read and write the contents of the shadow locations.

To understand why this is useful, consider a library that allocates an integer reference \( \ell \), and shares it with (untrusted) clients as an I/O buffer. Clients are expected to write only positive integers to \( \ell \), although the library does not strictly require this and the library’s algorithms can execute safely even if the integer is not positive. Over time, many clients of this library have been written. Now, suppose that the library is updated to use different algorithms that **really require \( \ell \) to always
makepub ≜ λ_. let tbl = ref bijempty in
          let sync = makesync() in
          (sync, tbl)

pubout ≜ λ(sync, tbl) r1.
          sync(_, bijlookup (!tbl) r1)

pubin ≜ λ(sync, tbl) r2.
          sync(_, bijlookup (bijinvert (!tbl)) r2)

pubwrap ≜ λm. membrane (pubout m) (pubin m)

pubin unwrap ≜ λm. membrane (pubout m) (pubout m)

pubref ≜ λmx1.
          let r1 = ref x1 in
          let r2 = ref (pubwrap m x1) in
          let (sync, tbl) = m in
          sync(_., tbl ← bijinsertnew (!tbl) r1 r2); r1

shadowread ≜ λmr. pubunwrap m (! (pubout m r))

shadowwrite ≜ λmr x. pubout m r ← pubwrap m x

Fig. 10. Public membrane implementation

be positive (else they crash). The obvious way to do this would be to rewrite the library to hold ℓ private, and to export two closures that read and write ℓ, the latter only after checking that the value being written is positive. However, this change breaks compatibility with all existing clients, since they must now be rewritten to invoke the new closures to access ℓ. The public membrane offers a general solution to this problem. Rather than export closures, the library can deploy a public membrane and declare ℓ as high-integrity. The membrane consistently replaces ℓ with a low-integrity shadow, say ℓ′, for the library’s clients. Importantly, the library’s clients don’t have to change. After a client updates ℓ′ (believing that it updated ℓ), the library can access ℓ′ using shadowread and copy it to ℓ if the updated value is a positive integer. Additionally, whenever the library updates ℓ internally, it can also copy the update to ℓ′ using shadowwrite. This way, the library can maintain its new invariant and retain complete compatibility with existing clients.

The functions comprising the public membrane are listed in Fig. 10.12 The expression makepub () creates a public membrane (consistently denoted m), which comprises a pair (sync, tbl) where the reference cell tbl contains a finite partial bijection on locations protected by (the lock buried in) sync. When a public membrane’s table sends location ℓ1 to ℓ2, we say that location ℓ1 is a (high-integrity) private location and location ℓ2 its (low-integrity) shadow location. The functions pubout and pubin transform between private and shadow locations by consulting the table. Both functions get stuck on locations not in the table. The functions pubwrap and pubunwrap lift these to transformations between values by applying the function membrane. Effectively, pubwrap replaces all private locations in the value passed to it with their shadow locations and pubunwrap does the opposite.

The expression pubref m v1 constructs a new private location initially containing value v1. In addition, it allocates a shadow location (called r2 in the code) that initially contains the low-integrity counterpart of v1. It stores an association between the two locations in m’s table. The shadow location r2 can be retrieved from the table by applying either pubout or pubwrap to the private location returned by pubref.

The function shadowread inspects a private location’s shadow location, converting its low-integrity contents into a high-integrity value using pubunwrap, whereas shadowwrite updates a private location’s shadow location after converting the given value to a low-integrity value using pubwrap.

To use this public membrane interface, the verified code first creates a new public membrane using makepub. Subsequently, it allocates private locations that might flow to untrusted code using

12We discuss the straightforward functions makesync, bijempty, bijinsertnew, bijlookup, and bijinvert in Appendix F.
the function \( pubref \) instead of the language construct \( \text{ref} \). Before sending any value to untrusted code, it invokes \( pubwrap \) to replace all nested private locations with their shadows. Dually, after receiving any value from untrusted code, it applies \( pubunwrap \) to replace nested shadow locations with corresponding private locations. At any point, the verified code can access shadow locations using \( \text{shadowread} \) and \( \text{shadowwrite} \). Appendix E shows an example of how the public membrane is used.

Public membrane specification. The OCPL specification of the public membrane is shown in Fig. 11. The assertion \( \text{ismembrane} \ y \ m \) associates a public membrane \( m \) to a logical name \( y \). The abstract predicate \( \text{isprivloc} \ y \ \ell \) represents knowledge that location \( \ell \) is a private location for the membrane named \( y \), i.e., \( \ell \) was previously allocated using \( pubref \) on the public membrane named \( y \). The assertion \( \text{isprivval} \ y \ v \) is defined as lift (\( \text{isprivloc} \ y \) \( \ell \)) by rule \( \text{IsPrivval} \). In particular, the assertion means that any location “extractable” from \( v \) is in the domain of \( y \)’s table. We call such values \( v \) private values.\(^{13}\)

The specification rules are straightforward, so we explain only some salient points here. The triple for \( pubref \) (rule \( \text{PubAllocSpec} \)) says that the application \( pubref \ m \ v \) returns a location \( \ell \leftrightarrow v \) together with the knowledge that \( \ell \) is a private location, represented by \( \text{isprivloc} \ y \ \ell \). It subsequently becomes the responsibility of the public membrane’s client, who owns \( \ell \leftrightarrow v \), to protect any high-integrity state reachable from \( \ell \)—for example, by keeping \( \ell \) hidden as we do in Appendix E. The triples \( \text{PubWrapSpec} \) and \( \text{PubUnwrapSpec} \) say that the function \( pubwrap \ m \) converts private values to low values, while \( pubunwrap \ m \) does the opposite. In particular, the output of \( pubwrap \), being low, can be freely shared with untrusted code. Also, \( pubunwrap \) has a non-progressive triple because unwrapping an arbitrary low value \( v_2 \) may apply \( pubin \ m \ell_2 \) with some low-integrity location \( \ell_2 \) unknown to \( m \), and our implementation of \( pubin \) gets stuck in such cases.\(^{14}\)

The implementation of the public membrane satisfies this specification. As an example, we briefly describe how we verify the \( pubwrap \) specification, \( \text{PubWrapSpec} \). First, we prove the following two lemmas showing that for a valid membrane \( m \), \( pubout \ m \) and \( pubin \ m \) produce functions that satisfy

\(^{13}\)Reasoning with private values is fairly straightforward using the definition in Fig. 3 and derived rules like \( \text{LiftApp} \) (§2.2).

\(^{14}\)For simplicity, we do not specify the functionality of \( pubwrap \) and \( pubunwrap \) beyond “returns a low, resp., private value”. More useful specifications would allow one to prove that, say, after wrapping private location \( \ell_1 \) twice and obtaining values \( v_2 \) and \( v'_2 \), there exists a low location \( \ell_2 \) such that \( v_2 = \ell_2 = v'_2 \).
the predicate ismon.

\[
\{ \text{ismembrane } \gamma m \} \ \text{pubout } m \{ f. \ \text{ismon progress } f \ (\text{isprivloc } \gamma) \ \text{lowloc} \} \\
\{ \text{ismembrane } \gamma m \} \ \text{pubin } m \{ f. \ \text{ismon noprogress } f \ \text{lowloc} (\text{isprivloc } \gamma) \}
\]

Next, we instantiate \text{MembraneSpec} (Fig. 9) with \(\Psi_1 = \text{isprivloc } \gamma\), \(\Psi_2 = \text{lowloc}\) and the two lemmas above to obtain

\[
\text{ismon progress pubwrap (isprivval } \gamma) \ \text{lowval}
\]

The triple \text{PubWrapSpec} follows by unfolding the definition of ismon (Fig. 9).

6 RELATED WORK

This paper focuses on the formal specification and verification of OCPs. While we know of only rather preliminary prior work in this space, a major point of our paper is to observe that the tools needed for effective verification of OCPs are already to a large extent available—the pieces just need to be assembled properly. In particular, our logic, OCPL, gets significant mileage out of existing verification techniques, notably robust safety and concurrent separation logic. In the following, we discuss related work on robust safety, the (limited amount of) existing work on specification of OCPs, and some other relevant work on object capabilities and ownership types.

\textit{Robust safety.} The concept of robust safety arose in the context of verifying security protocols that interact with adversaries. Early work used typing to prove “correspondence properties” for cryptographic protocols modeled in the spi calculus [Gordon and Jeffrey 2001]. In their work on the refinement type-checker F7, Bengtson et al. [2011] generalized robust safety to a richer class of integrity properties for a process calculus, RCF, with higher-order state. We inherit from their work the basic idea of using a notion of low-integrity values and proving robust safety, but the approaches differ greatly in detail. First, we show how to apply this idea to OCPs, a completely different domain. Second, we show how low-integrity values are directly encodable in modern separation logics, using a simple logical relation.

\textit{Object capabilities.} There has been only very preliminary work on specifying and verifying functional properties of object capabilities and OCPs. In his seminal paper on dynamic sealing, Morris [1973] proposed informal reasoning principles for programmers using dynamic sealing, but did not prove anything formally. Drossopoulou et al. [2015a] proposed predicates modeling trust and risk and used those predicates to specify a capability-based escrow exchange example [Miller et al. 2013]. They focused on this one example, whereas we develop general specifications for several OCPs. Further, they focus on syntactic specifications and do not define the semantics of their predicates. A subsequent manuscript [Drossopoulou et al. 2015b] bridges this gap to the semantics, but their Hoare logic seems inadequate for the examples we consider, e.g., it lacks a rule for dynamic allocation.

Perhaps the most closely related work to our own is that of Devriese et al. [2016]. As discussed in the introduction, they use a Kripke logical relation and a meta-property called effect parametricity to verify integrity properties for several examples of capability-wrapped user code in a language with higher-order state. There are several points of difference between our work and theirs. First, we work in a concurrent separation logic rather than directly in a low-level logical relation. As a result, in addition to being able to conduct our proofs at a much higher level of abstraction, we can give compositional specifications for higher-order object capability patterns (i.e., libraries), whereas they only verify specific programs that use object capabilities. We also exploit the notion of robust safety in verifying integrity properties of code that uses OCPs, whereas corresponding arguments only appear implicitly in their proofs. On the other hand, they develop semantic variants of the
so-called “reference graph properties” from the literature on object capabilities. These properties are important but they are also orthogonal to verification and, hence, we do not examine them. Last but not least, our proofs are machine-checked in Coq.

While specifying OCPs has received little attention so far, there has been a lot of other work on object capabilities and OCPs. Responding to renewed interest in dynamic sealing, Sumii and Pierce [2004] propose a bisimulation for proving contextual equivalences in a language with a dynamic sealing primitive. Roughly, the examples they consider are pairs of expressions—“modules” implementing the same “interface” using sealing—and the question they study is whether those expressions are indistinguishable, even if their internal representations differ. Bengtson et al. [2011] use dynamic sealing to define ideal implementations of cryptographic operations in RCF. They offer no general specifications for dynamic sealing analogous to the specification in §3, but derive instances of such a specification as needed. Van Cutsem and Miller [2013, §§4.3–4.4] describe a variant of our public membrane, which they use to implement proxy objects supporting so-called language invariants (such as the reasoning enabled, in JavaScript, by the ability to “freeze” object properties). Their focus is on the use of such membranes as an implementation technique, rather than on verification. Spiessens and Van Roy [2005]; Spiessens [2007] and Murray [2010] use, respectively, model- and refinement-checking tools to establish certain safety and liveness properties of abstract models of object capability systems, including some OCPs. To take one small example, Murray shows that a specific model of an unsealing operation does not reveal a sealed value unless a capability to that sealed value was passed (possibly indirectly) to the unsealing operation by the context. Although useful, such properties cannot be directly used to verify clients of the OCPs. In contrast, our goal is very different: we write compositional specifications for concrete implementations of OCPs and our specifications can be directly used to verify clients.

Ownership types. There are interesting similarities between the core mechanisms of OCPL and prior work on ownership types [Clarke et al. 2013]. In their seminal paper, Clarke et al. [1998] proposed a type system based on what came to be called owners-as-dominators. Roughly, the idea is to impose an ownership relation on objects, separating a public owner object from its hidden representation objects and ensuring that an owner mediates all outside access to its representation. Clarke et al. then proved that well-typed code preserves an invariant classifying data and enforcing isolation according to owners-as-dominators. In a similar vein, OCPL classifies locations as high-integrity (private) vs. low-integrity (public), and enforces that high-integrity locations cannot be accessed from low-integrity locations. However, OCPL is not a static type system, but rather a logic for verifying the enforcement of integrity properties in a dynamically-typed setting. Moreover, although OCPL requires that low locations contain low values, it does not stipulate any particular ownership discipline (like owners-as-dominators) for how the user should achieve this.

Other researchers have proved deeper semantic properties of owners-as-dominators. Banerjee and Naumann [2005a,b] prove relational parametricity theorems, using logical relations as a proof technique for showing that one representation may be safely replaced by another. Patrignani et al. [2011] show that an extension of owners-as-dominators can be used to prove relational secrecy properties for the join calculus, based on a distinction between high- and low-integrity values. In OCPL, we define low-integrity values using a simple (implicitly step-indexed) logical relation, and (like Patrignani et al.) our key meta-theorem concerns the interaction of user code with untyped, untrusted code. However, despite these similarities to prior work, our concrete goals are very different: rather than reasoning about relational properties, we focus on verifying functional specifications of OCPs and the robust safety of capability-wrapped code.
7 CONCLUSION AND FUTURE WORK

Object capability patterns (OCPs) enable programmers to enforce invariants on the private state of their objects, even when those objects are passed to untrusted code. In principle, this should make it easier to write secure and correct programs, but in practice, programmers may use OCPs incorrectly, resulting in subtle security flaws. In this paper, we develop OCPL, the first logic for compositionally specifying and verifying OCPs. We deploy it in reasoning about both implementations and representative clients of several well-known OCPs, in the context of a simple but expressive programming language with higher-order state.

We believe that using robust safety and separation logic to reason about OCPs scales to much richer settings. The Firefox web browser, for example, uses an automatic and significantly more sophisticated membrane pattern to enforce the so-called same-origin policy [Mozilla 2016; Barth 2011]. In ongoing work, we are exploring an extension of OCPL to reason about this system. Furthermore, while the Iris proof mode enables relatively high-level Coq proofs, such manual proofs are nonetheless often tedious and routine. Additional research is needed to scale such proofs up to realistic languages and improve automation.

A SEALING WITH LOW FUNCTIONS

In this appendix, we point out that, in the dynamic sealing OCP, representing proxy values as low-integrity functions renders unsealing non-deterministic, forcing somewhat surprising changes to otherwise “obviously safe” code.

Our implementation of sealing differs from Morris’ in one important respect. Ignoring synchronization, Morris sealed a value \( v \) by returning a function \( (\lambda k. \text{tbl} \leftarrow \text{mapinsertnew} (!\text{tbl}) k v) \) for extending the table.\(^{15}\) To unseal a value \( f \), Morris allocated a fresh location \( k \), applied \( f k \), and looked for \( k \) in the table. This simple change—returning a function rather than a location—renders

\[
\text{UnsealAnySpec} \quad \{ \text{isunseal } u \phi \} \ u \ v' \ \{ x. \text{issealed } γ \ x \ v' \ ϕ \}
\]

unsound. There are two problems. First, the triple makes no assumptions about the value \( v' \). When \( v' \) is a function \( f \), there is no way to safely apply \( f k \) as \( f \) might have “unfair” access to otherwise hidden state. An easy fix is to weaken the triple, assuming that \( v' \) is low so that, if \( v' \) is a function \( f \), we know by assumption that we can apply \( f k \) (if we can mark \( k \) low—we can). Second, the triple returns a value \( v \) such that \( \text{issealed } γ \ v \ v' \ ϕ \) which means that subsequent applications \( u \ v' \) must also return \( v \). This is absurd! An adversary with values \( f_1, f_2 \) obtained by sealing values \( v_1, v_2 \) can, for example, construct

\[
f \triangleq \text{let } r = \text{ref } \text{false} \text{ in } λk. \text{let } b = 1r \text{ in } (r \leftarrow (\text{not } b); (\text{if } b \text{ then } f_1 \text{ else } f_2) \ k)
\]

that, when unsealed, oscillates between \( v_1 \) and \( v_2 \). An easy fix is to weaken the triple further, giving up on deterministic unsealing.

We verified Morris’ implementation of sealing against a weaker specification, obtained by replacing rule \text{UnsealAnySpec} in Fig. 5 with

\[
\text{UnsealLowSpec} \quad \{ \text{isunseal } γ \ u \phi \ * \text{lowval } v' \} \ u \ v' \ \{ x. \phi x \},
\]

\(^{15}\)We are not so much interested in Morris’ implementation but in the fact that it returns a function. Other dynamic sealing implementations return functions and otherwise have attractive properties (e.g., dispensing with the table). Ignoring synchronization, the table-free implementation of sealing [Miller 2008; Taly et al. 2011]

\[
\text{let } r = \text{ref } \text{None} \text{ in } \text{let } \text{seal } = λx. \ r \leftarrow \text{Some } x \text{ in } \text{let } \text{unseal } = λf. \ (r \leftarrow \text{None}; \text{valOf } (!r)) \ \text{in } (\text{seal, unseal})
\]

shares this drawback with Morris’ implementation.
This switch to non-deterministic unsealing of low values comes at some cost. We must weaken the non-progressive triples in our intervals specification; for example, replacing $\text{MinAnySpec}$ by $\text{MinLowSpec}$:

$\{\text{ismin } \gamma \text{ imin } \text{lowval } \nu \} \text{ imin } \nu \{ \text{n, ret } \text{n. } \top \}$

With these weaker rules, we can no longer verify the function $\text{check} = \lambda j. \text{assert} (\text{imin } j \leq \text{imax } j)$ in our intervals client. Applying $\text{check}$ to a monster like the oscillating function $f$ can cause the assertion to fail. All is not lost, of course. We can rewrite $\text{check}$ to read $\text{check} = \lambda j. \text{let } j = \text{snap } j \text{ in assert} (\text{imin } j \leq \text{imax } j)$ after extending our intervals library with the trivial snapshot function $\text{snap} = \lambda x. \text{seal} (\text{unseal } x)$. The point of $\text{snap}$ is to replace an unpredictable function by a predictable one:

$\text{SnapSpec}$

$\{\text{issnap } \gamma \text{ snap } \ast \text{isinterval } \gamma \text{ n}_1 \text{ n}_2 \nu \} \text{ snap } \nu \{ \text{i. isinterval } \gamma \text{ n}_1 \text{ n}_2 \text{i} \}$

$\text{SnapLowSpec}$

$\{\text{issnap } \gamma \text{ snap } \ast \text{lowval } \nu \} \text{ snap } \nu \{ \text{i n}_1 \text{n}_2 , \text{ret i. isinterval } \gamma \text{ n}_1 \text{ n}_2 \text{i} \}$

$\text{SnapLow}$

$\text{issnap } \gamma \text{ snap } \vdash \text{lowval } \text{snap}$

With these changes, we can prove the assertion expression in our modified intervals client succeeds and the client is robustly safe.

### B PUBLIC-KEY INTERFACES FOR SEALING

In this appendix, we show that dynamic sealing can be used to implement ideal cryptographic signing/verification as well as encryption/decryption primitives, and that the specification of dynamic sealing (Fig. 5) can be specialized to derive very general specifications for these primitives. Such ideal primitives are sometimes used in the verification of cryptographic protocols [Bengtson et al. 2011]. While the observation that dynamic sealing can implement these cryptographic primitives is not new—Morris [1973] notes this even though he did not use the terms signing and encryption back then—the observation that specifications for the cryptographic primitives can be derived from those for dynamic sealing is new.

**Signature/verification.** A signature/verification primitive provides a function $\text{sign}$ that creates a low proxy for its argument. This proxy is usually called a signature. The proxy (signature) can be verified using a dual function $\text{verify}$, which when applied to the value returned by $\text{sign } \nu$, returns $\nu$ and if the argument was not the output of $\text{sign}$, gets stuck. The important point is how $\text{sign}$ and $\text{verify}$ are used in practice. In typical use, $\text{sign}$ is held private by a piece of code that has been verified to apply $\text{sign}$ only to values that satisfy a representation invariant $\phi$. The $\text{verify}$ function is publicly available to everyone and anyone can use it to verify signatures created by the code that holds $\text{sign}$. In this mode of use, signing/verification transfers knowledge of the representation invariant from the signer to the verifier: since the signer only signs values with representation invariant $\phi$, and $\text{verify}$ only returns previously signed values, the verifier always knows that any value returned by $\text{verify}$ must satisfy $\phi$.

It should be clear that $\text{sign}$ and $\text{verify}$ are quite similar to $\text{seal}$ and $\text{unseal}$ returned by $\text{makeseal}()$. The top half of Fig. 12 shows that, in fact, $\text{seal}$ and $\text{unseal}$ are an implementation of $\text{sign}$ and $\text{verify}$. The specification shown in this figure is a specific instance of the general sealing specification from Figure 5, derived by defining the abstract predicates $\text{issign}$, $\text{isverify}$, and $\text{issigned}$ to be $\text{isseal}$, $\text{isunseal}$, and $\text{issealed}$, respectively; using $\text{UnsealLow}$ to prove $\text{VerifyLow}$; and dropping $\text{SealLow}$. The derived specification says that $\text{makeseal}()$ returns a pair of functions that behave like $\text{sign}$ and $\text{verify}$ if the representation invariant $\phi$ implies lowval. This condition is necessary since $\text{verify}$
Asymmetric signatures.

\[
\text{MakeSignSpec} \quad \phi \text{ persistent} \quad (\forall v) \phi v \vdash \text{lowval } v
\]

\[
\{ \top \}
\]

\[
\text{makeseal }()
\]

\[
\{v_1, v_2, y, \text{ ret } (v_1, v_2). \text{ issign } y \phi v_1 * \text{isverify } y \phi v_2 \}
\]

\[
\text{SignSpec} \quad \{\text{issign } y \phi v \} \text{ sign } v \{x'. \text{ issigned } y v x' \phi\}
\]

\[
\text{VerifySpec} \quad \{\text{isverify } y \phi v \} \text{ verify } v' \{\text{ret } v. \top\}
\]

\[
\text{VerifyAnySpec} \quad \{\text{isverify } y \phi \} \text{ verify } v' \{x. \text{ issigned } y x v' \phi\}.
\]

\[
\text{VerifyLow} \quad \text{isverify } y \phi \vdash \text{lowval verify}
\]

\[
\text{SignedLow} \quad \text{issigned } y v v' \phi \vdash \text{lowval } v'
\]

\[
\text{SignedInv} \quad \text{issigned } y v v' \phi + \phi v
\]

\[
\text{SignedAgree} \quad \text{issigned } y v_1 v' \phi * \text{issigned } y v_2 v' \phi \vdash v_1 = v_2
\]

Asymmetric encryption.

\[
\text{MakeEncryptSpec} \quad \{ \top \}
\]

\[
\text{makeseal }()
\]

\[
\{v_1, v_2, y, \text{ ret } (v_1, v_2). \text{ isencrypt } y v_1 * \text{isdecrypt } y v_2\}
\]

\[
\text{EncryptSpec} \quad \{\text{isencrypt } y \phi v \} \text{ enc } v \{x'. \text{ isctext } y x v' \}
\]

\[
\text{DecryptSpec} \quad \{\text{isdecrypt } y \phi v \} \text{ dec } v' \{\text{ret } v. \top\}
\]

\[
\text{DecryptAnySpec} \quad \{\text{isdecrypt } y \phi\} \text{ dec } v' \{x. \text{ isctext } y x v' \}.
\]

\[
\text{EncryptLow} \quad \text{isencrypt } y \phi \vdash \text{lowval enc}
\]

\[
\text{CtextLow} \quad \text{isctext } y v v' \vdash \text{lowval } v'
\]

\[
\text{CtextAgree} \quad \text{isctext } y v_1 v' \phi * \text{isctext } y v_2 v' \phi + v_1 = v_2
\]

Fig. 12. Public-key interfaces (derived from Fig. 5)

returns previously signed values to untrusted code, so signed values should always be low—in cryptographic terms, signatures provide no secrecy. Additionally, the specification says that the value returned by verify always satisfies \(\phi\) (rule VerifyAnySpec), that verify itself is low (rule VerifyLow) so verify can be shared safely with untrusted code, and that the output of sign is low (rule SignedLow) so signatures can also be shared safely with untrusted code. On the other hand, sign itself is not low, so it should not be shared with untrusted code.

Encryption/decryption. An encryption/decryption primitive provides a function \(\text{enc}\) that creates a low proxy for its argument. A dual function \(\text{dec}\) converts the proxy back to the original argument. Typically, encryption/decryption is used by holding \(\text{dec}\) private in some piece of code, and making \(\text{enc}\) public. This allows anyone to encrypt a secret using \(\text{enc}\) and share it freely, with the guarantee that only the code holding \(\text{dec}\) can ever access the secret.
Again, \emph{enc} and \emph{dec} look similar to \emph{seal} and \emph{unseal} returned by \emph{makeseal()} and the bottom half of Fig. 12 formalizes this intuition by specializing the specification of Fig. 5 to match the intuitive description of encryption/decryption. The abstract predicates \emph{isencrypt}, \emph{isdencrypt}, and \emph{isctext} are defined to be \emph{isseal}, \emph{isunseal}, and \emph{issealed}, respectively. Importantly, the specification says that \emph{makeseal()} returns functions that behave like \emph{enc} and \emph{dec} (rule \texttt{MakeEncryptSpec}), that decrypting a previously encrypted value \emph{v} returns \emph{v} (rules \texttt{EncryptSpec} and \texttt{DecryptSpec}), and that the encryption function and ciphertexts are low (rules \texttt{EncryptLow} and \texttt{CtextLow}) so they can be shared with untrusted code. However, the decryption function is not low, so it should not be shared with untrusted code.

\section{Intervals Interface}

The following rules constitute the full specification of the intervals library in §3.

\textbf{Progressive triples.}

\begin{align*}
\texttt{IntervalsSpec} & \quad \{ \top \} \\
\texttt{intervals()} & \quad \{ v_1, v_2, v_3, v_4, \gamma, \text{ret } (v_1, v_2, v_3, v_4). \texttt{ismakeint } \gamma \, v_1 \ast \texttt{ismin } \gamma \, v_2 \ast \texttt{ismax } \gamma \, v_3 \ast \texttt{issum } \gamma \, v_4 \} \\
\texttt{MakeIntSpec} & \quad \{ \texttt{ismakeint' } \gamma \, n_1 \, f \} \\
\texttt{MINSpec} & \quad \{ \texttt{ismin } \gamma \, \text{imin } \ast \texttt{isinterval } \gamma \, n_1 \, n_2 \, i \} \quad \texttt{imin } \{ \text{ret } n_1. \top \} \\
\texttt{MAXSpec} & \quad \{ \texttt{ismax } \gamma \, \text{imax } \ast \texttt{isinterval } \gamma \, n_1 \, n_2 \, i \} \quad \texttt{imax } \{ \text{ret } n_2. \top \} \\
\texttt{SUMSpec} & \quad \{ \texttt{issum } \gamma \, \text{isum } \ast \texttt{isinterval } \gamma \, n_1 \, n_2 \, i \} \quad \texttt{isum } \{ f. \texttt{issum' } \gamma \, n_1 \, n_2 \, f \} \\
\texttt{SUM'Spec} & \quad \{ \texttt{issum' } \gamma \, n_1 \, n_2 \, f \ast \texttt{isinterval } \gamma \, n_1' \, n_2' \, i' \} \\
\texttt{f } & \quad i' \\
\texttt{INTERVALINV} & \quad \texttt{isinterval } \gamma \, n_1 \, n_2 \, i \ast \texttt{n_1 } \leq \texttt{n_2} \\
\texttt{INTERVALAGREE} & \quad \texttt{isinterval } \gamma \, n_1 \, n_2 \, i \ast \texttt{isinterval } \gamma \, n_1' \, n_2' \, i \\
& \quad i \ast \texttt{n_1 } = \texttt{n_1' } \ast \texttt{n_2 } = \texttt{n_2' }
\end{align*}

\textbf{Non-progressive triples.}

\begin{align*}
\texttt{MINAnySpec} & \quad \{ \texttt{ismin } \gamma \, \text{imin } \ast \texttt{interval } \gamma \, n_1 \, n_2 \, v \} \\
\texttt{MAXAnySpec} & \quad \{ \texttt{ismax } \gamma \, \text{imax } \ast \texttt{interval } \gamma \, n_1 \, n_2 \, v \} \\
\texttt{SUMAnySpec} & \quad \{ \texttt{issum } \gamma \, \text{isum } \ast \texttt{interval } \gamma \, n_1 \, n_2 \, v \}
\end{align*}
AnySpec
\{ \text{issum} \gamma n_1 n_2 f \} f v_2 \{ i n'_1 n'_2, \text{ret } i \}. \text{isinterval } \gamma (n'_1 + n'_1) (n_2 + n'_2) i \}?

Low values.

\begin{align*}
\text{IntervalLow} & : \text{isinterval } \gamma n_1 n_2 i \vdash \text{lowval } i \\
\text{Makeint’Low} & : \text{ismakeint’ } \gamma n_1 f \vdash \text{lowval } f \\
\text{MakeintLow} & : \text{ismakeint } \gamma mk \vdash \text{lowval } mk \\
\text{MinLow} & : \text{ismin } imin \vdash \text{lowval } imin \\
\text{MaxLow} & : \text{ismax } imax \vdash \text{lowval } imax \\
\text{Sum’Low} & : \text{issum’ } \gamma n_1 n_2 f \vdash \text{lowval } f \\
\text{SumLow} & : \text{issum } isum \vdash \text{lowval } isum
\end{align*}

D BLOCKING CARETAKERS

In this appendix, we briefly present a simpler implementation of API caretakers:\footnote{We discuss the straightforward functions \text{makelock’}, \text{release}, \text{acquire}, and \text{syncwith} in Appendix F.}

\begin{align*}
\text{makecaretaker} & \triangleq \text{makelock’} \\
\text{enable} & \triangleq \text{release} \\
\text{wrap} & \triangleq \lambda \text{ct } f \ x. \ \text{syncwith ct } (\lambda -. f x) \\
\text{disable} & \triangleq \text{acquire}
\end{align*}

The idea is that, if we are happy to let wrappers block until a caretaker is enabled, we can dispense with the \text{enabled} flag used in §4. In this implementation, a caretaker is a lock. The function \text{makelock’} allocates a fresh lock, initially locked. The function \text{syncwith} is analogous to \text{sync}, except that it takes the lock to use as an initial argument. To disable and enable wrappers, we simply acquire and release the lock they need. This implementation also satisfies the API caretaker specification (Fig. 7).

E PUBLIC MEMBRANE CLIENT

In this appendix, we further illustrate the public membrane by describing a simple client program that uses it. First, we define the following auxiliary function, \text{getint}. This function presupposes that we have some invariant on a private integer location, \( r \), and that we want to periodically update \( r \) by “merging” its contents with those of its shadow location, using some merge function \( f \) that preserves the invariant.

\begin{align*}
\text{getint} & \triangleq \lambda m \ f \ r. \ \text{let } n_1 = ! r \ \text{in} \ \text{let } x_2 = \text{shadowread } m \ r \ \text{in} \\
& \quad \text{if isint } x_2 \ \text{then} \\
& \quad \quad \text{let } n_3 = f \ n_1 \ x_2 \ \text{in} \\
& \quad \quad \text{let } _{-} = \text{if } n_1 \neq n_3 \ \text{then } r \leftarrow n_3 \ \text{else } () \ \text{in} \\
& \quad \quad \text{let } _{-} = \text{if } x_2 \neq n_3 \ \text{then } \text{shadowwrite } m \ r \ n_3 \ \text{else } () \ \text{in} \\
& \quad \quad n_3 \\
& \quad \quad \text{else } (\text{shadowwrite } m \ r \ n_1; n_3)
\end{align*}

If the private location \( r \) and its shadow contain integers \( n_1 \) and \( n_2 \), the code applies \( f \ n_1 \ n_2 \) to obtain the “merged” integer \( n_3 \), updates \( r \) and its shadow, and returns \( n_3 \); otherwise, the code overwrites the shadow’s contents with (and returns) \( n_1 \).

Our illustrative client program is a private up/down counter with increment and decrement functions, and private lower and upper limits. The invariant we have in mind is that the counter always remains within these limits. However, the counter also exposes shadow locations for the lower and upper limits to its untrusted context. The context can freely update these shadow lower
and upper limits. However, these changes are propagated to the private locations (using \texttt{getint}) only if the changes maintain the intended invariant.

\begin{verbatim}
client \symbol{61} \texttt{let} \texttt{m} = \texttt{makepub()} \texttt{in}
\texttt{let} \texttt{lo} = \texttt{pubref} \texttt{m} \texttt{0} \texttt{in} \texttt{let} \texttt{c} = \texttt{ref} \texttt{0} \texttt{in} \texttt{let} \texttt{hi} = \texttt{pubref} \texttt{m} \texttt{0} \texttt{in}
\texttt{let} \texttt{sync} = \texttt{makesync()} \texttt{in}
\texttt{let} \texttt{use} = \lambda_. \texttt{sync}(\lambda_. \texttt{assert} \texttt{!lo} \leq !\texttt{c}; \texttt{assert} \texttt{!c} \leq !\texttt{hi})
\texttt{let} \texttt{getlimits} = \lambda_. \texttt{let} \texttt{n} = !\texttt{c} \texttt{in}
\texttt{let} \texttt{a} = \texttt{getint}(\lambda n_1 n_2. \texttt{if} n_2 \leq \texttt{n} \texttt{then} n_2 \texttt{else} n_1) \texttt{lo} \texttt{in}
\texttt{let} \texttt{b} = \texttt{getint}(\lambda n_1 n_2. \texttt{if} \texttt{n} \leq n_2 \texttt{then} n_2 \texttt{else} n_1) \texttt{hi} \texttt{in}
(a, b)
\texttt{let} \texttt{decr} = \lambda_. \texttt{sync}(\lambda_. \texttt{let} \texttt{n} = (!\texttt{c}) - 1 \texttt{in}
\texttt{let} \texttt{b} = \texttt{fst}(\texttt{getlimits}()) \leq \texttt{n} \texttt{in}
\texttt{if} \texttt{b} \texttt{then} \texttt{c} \leftarrow \texttt{n} \texttt{else} (;b)
\texttt{let} \texttt{incr} = \lambda_. \texttt{sync}(\lambda_. \texttt{let} \texttt{n} = (!\texttt{c}) + 1 \texttt{in}
\texttt{let} \texttt{b} = \texttt{n} \leq \texttt{snd}(\texttt{getlimits}()) \texttt{in}
\texttt{if} \texttt{b} \texttt{then} \texttt{c} \leftarrow \texttt{n} \texttt{else} (;b)
\texttt{let} \texttt{lo'} = \texttt{pubwrap} \texttt{m} \texttt{lo} \texttt{in} \texttt{let} \texttt{hi'} = \texttt{pubwrap} \texttt{m} \texttt{hi} \texttt{in}
(use, lo', hi', incr, decr)
\end{verbatim}

The \texttt{client}'s private state comprises a public membrane \texttt{m}, a private counter \texttt{c} and private limits \texttt{lo} and \texttt{hi}, subject to the representation invariant \texttt{!lo} \leq !\texttt{c} \leq !\texttt{hi} (i.e., the counter respects its limits). The \texttt{client} returns (i) a simple function \texttt{use} that, when applied, simply asserts the representation invariant (and that could be extended to offer some service to the counter's clients), (ii) the shadow locations \texttt{lo'} and \texttt{hi'} that substitute \texttt{lo} and \texttt{hi} for the surrounding untrusted code (the untrusted code may freely change these at any time) and (iii) increment and decrement functions, \texttt{incr} and \texttt{decr}, that either change the counter \texttt{c} and return \texttt{true} or (when changing the counter would violate its current limits) return \texttt{false}. Prior to changing the counter, \texttt{incr} and \texttt{decr} copy the shadow locations \texttt{lo'} and \texttt{hi'} into \texttt{lo} and \texttt{hi} using the function \texttt{getint}, if doing so will not break the representation invariant.

Using the rules of OCPL, we prove that \texttt{client} is robustly safe, meaning that no context can exploit the returned values \texttt{use}, \texttt{incr}, \texttt{decr}, \texttt{lo'} and \texttt{hi'} in a way that violates the assertions about the representation invariant in \texttt{use}. To do this, we first prove that \texttt{client} satisfies the following triple: \{ \top \} \texttt{client} \{ x. \texttt{lowval} x \}. One key step in this proof is showing that \texttt{lo'} and \texttt{hi'} are both low. This follows because \texttt{lo'} and \texttt{hi'} are obtained from \texttt{pubwrap} and the postcondition of \texttt{pubwrap} (rule \texttt{PubWrapSpec}, Fig. 11) says that the value it returns is low. Robust safety follows immediately from \texttt{Theorem RobustSafety} applied to this triple.

\section{Library Functions}

In this appendix, we specify the implementations of locks, finite maps, and finite bijections used in our examples. As nothing here is original or terribly interesting, we relegate many implementation and verification details to our Coq development.
Initially locked locks.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LockedExclusive</td>
<td>locked γ * locked γ ⊢ ⊥</td>
</tr>
<tr>
<td>MakeLockSpec</td>
<td>{ T } makelock’ () { lk γ, ret lk. islock γ lk R * locked γ }</td>
</tr>
<tr>
<td>ReleaseSpec</td>
<td>{ islock γ lk R * locked γ * R } release lk { ret (). T }</td>
</tr>
<tr>
<td>AcquireSpec</td>
<td>{ islock γ lk R } acquire lk { ret (). locked γ * R }</td>
</tr>
</tbody>
</table>

Initially unlocked locks.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MakeLockSpec</td>
<td>{ R } makelock () { lk γ, ret lk. islock γ lk R }</td>
</tr>
</tbody>
</table>

Synchronization.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IsSync</td>
<td>issync sync R ≜ □ \forall Q. { R } e { v. R * Q } → sync (λ_. e) { v. Q }</td>
</tr>
<tr>
<td>SyncWithSpec</td>
<td>{ islock γ lk R } syncwith lk { v. issync v R }</td>
</tr>
<tr>
<td>MakeSyncSpec</td>
<td>{ R } makesync () { v. issync v R }</td>
</tr>
</tbody>
</table>

Fig. 13. Lock and synchronization interface

**Locks and synchronization.** We specify locks and synchronization in Fig. 13. Rules LockedExclusive–AcquireSpec constitute a CAP-style lock specification [Dinsdale-Young et al. 2010] satisfied by, for example, the evident implementation of spin locks using CAS. The assertion islock γ lk R represents knowledge that the value lk is a lock with abstract name γ protecting resource R. The assertion locked γ represents ownership of the lock named γ. Thus, for any resource R,

- makelock’ () returns a new, locked lock lk protecting R (MakeLock’Spec);
- release lk gives up lock lk and resource R, returning unit (ReleaseSpec); and
- acquire lk grabs lock lk and the resource R it protects, returning unit (AcquireSpec).

This specification is atypical in that makelock’ constructs a locked lock, a feature needed only to argue that our caretaker specification is just a specialized lock spec (see the implementation of “blocking caretakers” in Appendix D). MakeLockSpec embodies a typical CAP-style lock specification: it specifies the evident wrapper around makelock’ and release that consumes resource R in order to construct a new, unlocked lock lk protecting resource R.

Rules IsSync–MakeSyncSpec specify the following simple library, readily verified against any lock implementation.

\[
\text{syncwith} ≜ \lambda lk f. \text{acquire lk}; \text{let } r = f () \text{ in release lk}; r
\]

\[
\text{makesync} ≜ \lambda _. \text{let } lk = \text{makelock () in syncwith lk}
\]

Given a lock lk and a thunk f, the function syncwith applies f while holding the lock, returning whatever f () returns. The function makesync returns syncwith lk for a fresh lock lk. In specifying makesync, we follow Turon et al. [2013]. Definition IsSync is the key. It says that to prove sync (λ_. e) returns a value satisfying Q, it suffices to show that e, when given access to the resource R protected by sync’s lock, (i) returns a value satisfying Q and (ii) preserves R.
Finite maps. We specify functional finite maps in Fig. 14. The spec is parameterized by an injection \( \iota : X \rightarrow \text{Val} \) from some type \( X \) (our examples use locations) to values. The assertion

\[
ismap \ \map
\]

denotes knowledge that value \( \map \) represents the finite partial function \( f : X \rightarrow \text{Val} \). \text{MapEmptySpec} says that value \( \mapempty \) represents the empty map. \text{MapInsertNewSpec} specifies a special case of insertion. \text{MapLookupPartialSpec} specifies a partial lookup operation. The evident implementation of finite maps using association lists satisfies this spec when \( X \) enjoys decidable equality.

Finite bijections. We specify functional finite partial bijections in Fig. 15. As with finite maps, the spec is parameterized by an injection \( \iota : X \rightarrow \text{Val} \) from some type \( X \) to values. The assertion

\[
isbij \ \bij
\]

denotes knowledge that value \( \bij \) represents the finite partial bijection \( f, f' : X \rightarrow \text{Val} \) in the sense that for every \( x \in X \) and value \( \nu' \), if \( f x = \nu' \), then there exists \( x' \in X \) such that \( \nu' = \iota x' \) and \( f' x' = \iota x \). Representing a bijection as a pair of finite maps (as specified in Fig. 14) leads to a natural implementation of this specification.

ACKNOWLEDGMENTS

This research was supported in part by a Microsoft Research PhD Scholarship, and in part by a European Research Council (ERC) Consolidator Grant for the project “RustBelt”, funded under the European Union’s Horizon 2020 Framework Programme (grant agreement no. 683289). We wish to thank Andrea Fischer and the OOPSLA reviewers for extremely helpful and detailed feedback.
REFERENCES


