Probabilistic Relational Verification for Cryptographic Implementations

Gilles Barthe\textsuperscript{1} Cédric Fournet\textsuperscript{2} Benjamin Grégoire\textsuperscript{3}

Pierre-Yves Strub\textsuperscript{1} Nikhil Swamy\textsuperscript{2} Santiago Zanella-Béguelin\textsuperscript{2}

IMDEA Software Institute\textsuperscript{1} Microsoft Research\textsuperscript{2} INRIA\textsuperscript{3}

\{gilles.barthe,pierre-yves.strub\}@imdea.org, \{fournet,nswamy,santiago\}@microsoft.com, benjamin.gregoire@sophia.inria.fr

Abstract

Relational program logics have been used for mechanizing formal proofs of various cryptographic constructions. With an eye towards scaling these successes towards end-to-end security proofs for implementations of distributed systems, we present \( \text{RF}^* \), a relational extension of \( \text{F}^* \), a general-purpose higher-order stateful programming language with a verification system based on refinement types. The distinguishing feature of \( \text{RF}^* \) is a relational Hoare logic for a higher-order, stateful, probabilistic language. Through careful language design, we adapt the \( \text{F}^* \) typechecker to generate both classic and relational verification conditions, and to automatically discharge their proofs using an SMT solver. Thus, we are able to benefit from the existing features of \( \text{F}^* \), including its abstraction facilities for modular reasoning about program fragments. We evaluate \( \text{RF}^* \) experimentally by programming a series of cryptographic constructions and protocols, and by verifying their security properties, ranging from information flow to unlinkability, integrity, and privacy. Moreover, we validate the design of \( \text{RF}^* \) by formalizing in Coq a core probabilistic \( \lambda \)-calculus and a relational refinement type system and proving the soundness of the latter against a denotational semantics of the probabilistic \( \lambda \)-calculus.

Categories and Subject Descriptors D.3.1 [Programming Languages]: Formal Definitions and Theory—Semantics; D.2.4 [Software Engineering]: Software/Program Verification.

Keywords program logics; probabilistic programming

1. Introduction

Many fundamental notions of security go beyond what is expressible as a property of a single execution of a program. For example, non-interference [25], the property underlying information-flow security, relates the observable behaviors of two program executions. Recognizing the importance to computer security of such hyperproperties [20], researchers have developed a range of program analyses and verification tools for proving relations between two or more programs, or two or more executions of the same program. For instance, Benton’s relational Hoare logic [11] generalizes Hoare logic to reason about properties of two programs.

In addition, security properties must often account for probabilistic behaviors. For instance, in cryptography, simulation- and indistinguishability-based notions of security are specified in terms of the probability that an adversary wins in some probabilistic experiment. Starting from Kozen’s seminal work [30], many logics for reasoning about probabilistic programs have been developed.

Recently, these two lines of work have been combined into a relational program logic called \( p\text{RHL} \) for reasoning about probabilistic imperative programs [7]. This logic can justify common patterns of probabilistic reasoning about hyperproperties used in cryptographic proofs, including observational equivalence, equivalence up to failure and reductionist arguments. \( p\text{RHL} \) forms the backbone of \textit{EasyCrypt} [8], a tool-assisted framework which has been used for verifying the security of encryption and signature schemes, modes of operation for block-ciphers, and hash function designs in the computational model. These advances, among others, raise the prospect of a new class of verifiably secure systems: those that are proven secure based on standard computational assumptions (such as the existence of one-way functions) and whose verification encompasses all aspects of the system implementation.

\( \text{RF}^* \): \textit{end-to-end security of cryptographic implementations} In an effort to scale logics like \( p\text{RHL} \), towards end-to-end security proofs of system implementations, this article presents a new language called \( \text{RF}^* \), building on \( \text{F}^* \) [45], a dependently typed dialect of ML. \( \text{F}^* \), and its predecessor \( \text{F7} \) [12], make use of refinement types to verify implementations scaling to tens of thousands of lines of code, including the Transport Layer Security Internet standard (TLS) [13], multi-party sessions, web-browser extensions, zero-knowledge protocols, and the \( \text{F}^* \) typechecker itself.

\( \text{RF}^* \) integrates within \( \text{F}^* \) an expressive system of relational refinements to support fine-grained reasoning about probabilistic computations. Through careful language design, we are able to use the relational features of \( \text{RF}^* \) in smooth conjunction with the existing features of \( \text{F}^* \), allowing the large corpus of already-verified \( \text{F}^* \) code to be reasoned about effectively when used in a relational context. As such, our work opens the door to semi-automated security verification through relational refinement types, instead of a somewhat inflexible combination of parametricity and type safety (as in \( \text{F7} \)), or through detailed tactic-based interactive proofs (as in \textit{EasyCrypt}), as a basis for certifying the security of critical pieces of Internet infrastructure, such as a reference implementation of TLS.

Technically, this paper makes three broad contributions:

\footnote{This work has been partially supported by the Amarout European Program.}
1. A relational logic for higher-order stateful probabilistic programs: we formalize in the Coq proof assistant \( \lambda_0 \), a lambda calculus with references, random sampling, and unbounded recursion. We develop a relational refinement type system for \( \lambda_0 \), and prove it sound with respect to a denotational interpretation of judgments as relations over pairs of store-passing probabilistic functions. To our best knowledge, \( \lambda_0 \) is the first relational logic for higher-order stateful probabilistic programs. (§3)

2. The design and implementation of \( R^* \): \( \lambda_0 \) forms the basis of the design of \( R^* \), an extension of \( F^* \). We show how to encode relational refinement types within a new relational state monad, R DST. We provide a type inference algorithm for R DST, in the form of a weakest pre-condition calculus that computes relational verification conditions. Proofs of these verification conditions can be discharged automatically by the \( R^* \) typechecker and the Z3 [21] SMT solver. (§4)

3. An experimental evaluation of \( R^* \): we demonstrate the expressiveness of \( R^* \) through a representative set of examples, starting from simple (non-probabilistic) information flow, and gradually moving towards more advanced cryptographic models and systems. To date, we have used \( R^* \) to automatically verify a total of around 1,400 lines of code for a variety of relational properties, ranging from termination-insensitive non-interference to various indistinguishability-based properties for encryption, besides others. Several examples make essential use of higher-order and stateful features of \( R^* \), emphasizing the utility of the \( \lambda_0 \) logic for practical security verification. (§2 and §5)

The \( \lambda_0 \) theory formalized in Coq, the \( R^* \) compiler, and all the example programs mentioned in this paper are available online from http://research.microsoft.com/fstar.

2. Programming with relational refinements

We start by describing \( R^* \) informally through a series of examples, beginning with a brief introduction to \( F^* \) itself, and then focusing on the main new feature in \( R^* \), i.e., relational refinement types.

2.1 From classic to relational refinements. \( F^* \) is a call-by-value higher-order programming language with primitive state and exceptions, similar to ML, but with a more expressive type system based on dependent refinement types. Refinement types are written \( \texttt{x:t(\phi)} \) where \( \phi \) is a logical formula. For instance, the code fragment below defines a refined type for non-negative integers, then for integers modulo some number \( p \):

\[
\begin{align*}
type \texttt{nat} &= \texttt{nnat} \{ 0 \leq n \} \\
type \texttt{mod} p &= \texttt{nnat} \{ n < p \} \\
let \texttt{p} &= 97 \\
let \texttt{n : mod p} &= 73
\end{align*}
\]

Typechecking \( F^* \) programs involves logical proof obligations, which are delegated to the Z3 SMT solver. For instance, to check that \( n \) has type \( \texttt{mod p} \), the \( F^* \) typechecker emits the proof obligation \( p = 97 \Rightarrow 0 \leq 73 < p \), which is easily discharged by Z3. Type safety means that, whenever an expression \( e \) with type \( \texttt{x:t(\phi)} \) reduces to a value \( v \), this value \( v \) satisfies the formula \( \phi[v := v] \). The type system provides structural subtyping. For instance, \( \texttt{nat} \) is a subtype of \( \texttt{int} \), and \( \texttt{mod p} \) is a subtype of \( \texttt{mod q} \) when \( p \leq q \). These subtyping relations are automatically proved and applied by \( F^* \).

Refinements can be combined with dependent function types, written \( \texttt{x:t->t'} \), where the formal parameter \( \texttt{x} \) is in scope in the result type \( \texttt{t'} \). We also use dependent pairs, written \( \texttt{x:*t'} \), where the variable \( x \) of the first component is in scope in the type \( \texttt{t'} \) of the second component. For instance, we may write and typecheck addition modulo as follows (where the refinement braces bind tighter than the arrow):

\[
\begin{align*}
\texttt{val add : \texttt{p:nat -> x:mod p -> y:mod p -> z:mod p} \{ \{ x \times y \mod p \} \}} \\
\texttt{let add \texttt{p x y} \texttt{=} \texttt{let s \texttt{=} \texttt{x+y} \texttt{if is < p then s else s-p}}
\end{align*}
\]

\( F^* \) also provides primitive support for programming with state. For example, one may write let \( \texttt{incr} \texttt{i} \texttt{=} \texttt{i+1} \texttt{if is < p} \texttt{then s else s-p} \). By combining refinements with references, one can express invariants on the program state, e.g., \( \texttt{ref nat} \) is the type of mutable locations that contain non-negative integers. To describe more precise properties of effectful programs, \( F^* \) provides more advanced mechanisms, including a monadic mode [46], where one can reason about programs using variants of the Hoare state monad of Nanevski et al. [34] together with McCarthy’s select/update theory for modeling the heap [32]. For example, one can give \( \texttt{inc} \) a specification of the form \( \texttt{inc nat} \Rightarrow \texttt{ST (Ah,True) unit} \{ \lambda h \rightarrow h'.=\texttt{Upd h i (1 + Sel h i)} \} \), where \( \texttt{ST pre post} \) can be understood as the state-passing function \( h:\texttt{heap} \Rightarrow \texttt{(x+1,heap\{post h \times h'})} \) although, in reality, \( F^* \) provides primitive inference for state. That is, the type of \( \texttt{inc} \) states a trivial pre-condition on the input heap \( h \), and a post-condition indicating that the final heap \( h' \) differs from \( h \) at the location \( i \), which is incremented. \( F^* \) provides type inference in the form of a higher-order weakest pre-condition calculus to help ease the burden of writing such precise specifications [46].

\( R^* \) extends \( F^* \) with relational refinements: a type can (also) be decorated with a relational formula, placed within double braces \( \{ \ldots \} \), that specifies a joint property on pairs of values. Relational formulas can independently refer to the \textit{left} and \textit{right} values of every program variable in scope, using the projections \( L \) and \( R \), respectively; projections extend naturally to arbitrary formulas. Intuitively, for deterministic programs, type safety means that, whenever we obtain two results \( \texttt{vL} \) and \( \texttt{vR} \) by evaluating an expression \( e : \texttt{x:t(\phi)} \) in two contexts that provide well-typed substitutions for \( e \)'s free variables, then the formula \( \phi[L x := vL \{ R x := vR \}] \) is valid. More generally, instead of considering two executions of the same program, \( R^* \) allows proving relations between the results of two programs, i.e., we relate \( \texttt{vL} \) and \( \texttt{vR} \) at a (relationally refined) type using \( \texttt{vL} \Rightarrow \texttt{vR} : \texttt{t} \). We write \( \texttt{e : t} \) as a shorthand for \( \texttt{e \Rightarrow e : t} \).

We start with a few simple examples. Take the expression \( e \) to be \( z - z \); we can give the type \( \texttt{x:int(\{L x + R x\})} \), meaning that for any pair of substitutions \( \sigma_L \) and \( \sigma_R \), evaluating \( \sigma_L e \) yields the same result as evaluating \( \sigma_R e \). Similarly, we have \( x + x + x : \texttt{int(\{L x + R x \Rightarrow L x + R x + L x\})} \), stating a simple equivalence between two integer expressions evaluated with the same value for \( x \).

Relational refinements can also be used to describe properties beyond equivalence. For example, we can express the type of monotonic integer functions as \( \texttt{x:int -> y:int(\{L x \leq R x \Rightarrow L y \leq R y\})} \) and the type of \( k \)-sensitive integer functions, for some metric \( \texttt{dist} \), as \( \texttt{x:int -> y:int(\{\texttt{dist(L x)}(R y) \leq k \times \texttt{dist(L x)}(R x)\})} \).

\( R^* \) can automatically check (by subtyping) that a function such as \( \texttt{fun x -> k \times x} \) is both monotonic and \( k \)-sensitive for any \( k \geq 0 \).

Relational refinements are strictly more expressive than plain refinements: one can encode any plain refinement \( \{ \phi \} \) as the relational refinement \( \{ \{ L \phi \land R \phi \} \} \) that independently specifies \textit{left} and \textit{right} properties. For instance, the type \( \texttt{nat} \) above is automatically desugared to \( \texttt{nnat(\{0 \leq n \land n \leq R n\})} \). Pragmatically, this enables us to mix property refinements and relational refinements in our concrete syntax, and to import any refinement-typed \( F^* \) library in relational mode by applying the encoding. When authoring programs with specific relational properties in mind, one need issue only a single compiler directive (aka a pragma) to switch the verifier to relational mode. We contend that the resulting language, \( R^* \), brings relational program verification out of the domain of tools applied to small fragments of pseudocode with interactive proofs, to a practical programming language suitable for small- to medium-scale systems implementations.
2.2 Information flow. Relational refinements can be systematically used to give a semantic characterization of termination-insensitive non-interference [41]. Whereas standard type-based information flow controls resort to security labels and ad hoc syntactic mechanisms to conservatively determine when the observable outputs of a program may depend on its secret inputs, RF* can directly verify the corresponding equivalences, as illustrated below.

Recall that non-interference means that public results do not depend on secrets. If an expression e with base type a that computes over some secret information can be given the type \( \text{type } e : a = x : a \) \((L x = R x)\), then its result can be safely published, since the execution of e reveals no information about the secrets.

Capturing the intuition from labelled information flow type systems with “high” and “low” confidentiality levels, we use the type \( \text{type } e : a \) (the type of values that are “equal on both sides”) for low-confidentiality values, and also written low a. In contrast, we use the type a (the type of unrelated left and right values) for high-confidence values, writing hi a as an alias for a. As usual, low a is a subtype of hi a, meaning that public values can be treated as secret, but not the converse.

Using these type abbreviations, we can write programs such as \( \text{fun } (x, y) \rightarrow (x + y, x + 1) \) and give them information flow types such as \( \text{hi int \rightarrow low int \rightarrow hi int \rightarrow low int} \). More interestingly, we can supplement these types with relational refinements that capture more flexible information-flow policies. For example, a plausible confidentiality policy for credit card numbers conceals all but their last four digits, as specified and implemented below.

\[
\text{val last4: n:hi int \rightarrow int2string (n \% 10000)} \rightarrow \text{L s = R s} \]

\[
\text{let last4 n = \"********\" \text{int2string (n \% 10000)} \}
\]

Tracking leaks via control dependencies (aka implicit flows) is a characteristic feature of information flow type systems. To illustrate how RF* reasons about implicit flows, consider the program \( \text{fun b \rightarrow if b then e else e'} \). Assuming that b is secret, flow-insensitive type systems would conservatively give this program the type \( \text{hi bool \rightarrow low a} \). To give this program the more precise type \( \text{hi bool \rightarrow low a} \), we need to analyze four cases that arise from applying this function twice to arbitrary boolean arguments L b and R b, and prove that the results in all cases are the same. The four typechecking goals are

- \( e : \text{low a} \), assuming \( L b = R b \) and \( b = \text{true} \);
- \( e' : \text{low a} \), assuming \( L b = R b \) and \( b = \text{false} \);
- \( e = e' : \text{low a} \), assuming \( L b = \text{true} \) and \( R b = \text{false} \); and
- \( e' \sim e : \text{low a} \), assuming \( L b = \text{false} \) and \( R b = \text{true} \).

Anticipating on the next section, our proof rules for relating two values v0 and v1 are relatively simple. Proving \( v_0 \sim v_1 : \text{xt}([\phi]) \) involves first proving \( v_0 \sim v_1 : \text{t} \) (which for base types simply means that both v0 and v1 have type t), and then proving \( \phi[L x, R x := v_0, v_1] \). So, RF* can easily prove, for instance,

\[
\text{(fun b \rightarrow if b then 0 else 0) : hi bool \rightarrow low int and (fun x \rightarrow if x = 0 then 0 else 0) : hi int \rightarrow low int}
\]

even though, syntactically, those functions branch on confidential values. For expressions, particularly those that have side effects, the problem is more complex. Our strategy is to adapt the Hoare monad \( \text{ST pre \ post} \) provided by F* to a relational version called \( \text{RST} \), where \( \text{RST pre \ post} \) can be seen as the type shown below:

\[
\text{h:heap}\{\text{pre } (L h) (R h)\} \rightarrow \text{xt} + h'.\text{heap}\{\text{post } (L h) (R h) (L x) (R x) (L h') (R h')\}\}
\]

This is the type of pairs of functions that, when run in a pair of input heaps \( L h \) and \( R h \) satisfying the 2-place relational pre-condition predicate \( \text{pre} \), may diverge, but if they both converge, yield results \( L x \) and \( R x \) and output heaps \( L h' \) and \( R h' \) that satisfy the 6-place relational post-condition predicate \( \text{post} \).

Using the \( \text{RST mono} \) and its associated weakest pre-condition calculus, we can type the following program, which branches on a confidential value and then performs matching public side-effects:

\[
\text{val x:ref int \rightarrow b:bool \rightarrow RST (\lambda_\_ True) unit post where post h0 h1 \_ h0' h1' = L x=R x \wedge h0\_h1 \Rightarrow h0'=h1' \}
\]

\[
\text{let f x b = if b then x := 1 else x := 1} \]

RF* infers a weakest pre-condition predicate transformer for this program, then checks that it is consistent with any programmer supplied annotation (the annotation is optional for loop-free programs). In our example, the pre-condition of f states that it can run in any pair of heaps, while its post-condition ensures that, if \( f \) is applied twice to the same references in the same heaps, then regardless of its boolean argument, the resulting heaps are also the same, i.e., the type reveals that \( f \) does not leak information despite having side-effects guarded by a secret boolean.

More complex programs, for example those that may leak information via side-effects based on aliasing, can be verified similarly:

\[
\text{val g: x:ref int \rightarrow y:ref int \rightarrow b:bool \rightarrow RST (\lambda_\_ True) unit post where post h0 h1 \_ h0' h1' = L x=R y \wedge R x=R y \Rightarrow \text{Sel} h0' (L y)=\text{Sel} h1' (R y) \}
\]

\[
\text{let g x y b = if b then x := 1 else y := 1; x := 0} \]

The type of g states that, if \( x \) and \( y \) are not aliased, then the final contents of the reference are the same.

Thus, the expressiveness of RF*, combined with its ability to use Z3 to discharge proof obligations, enables automated reasoning in the style of a relational Hoare logic for proving non-interference properties of higher-order stateful programs.

2.3 Sampling, chosen-plaintext security, and one-time pads. We introduce probabilistic relational reasoning in RF* using symmetric encryption schemes. Our goal is to communicate encrypted messages between a sender and a receiver without leaking any information about their content. (From an information flow viewpoint, ciphertexts are public, whereas plaintexts are secret.) For simplicity, we assume that messages range over byte arrays with a fixed size \( n \) (called blocks) and we do not consider active attackers. Padding and authentication against chosen-ciphertext attacks can be easily added, but would complicate our presentation (see §5 for a description of our model for chosen-ciphertext security).

We assume that the sender and the receiver share a secret key \( k \) (also a block), sampled uniformly at random by calling the primitive function \( \text{sample} \). We model this assumption by writing a single program where both parties are within the scope of this key. The simplest secure encryption scheme is the one-time pad, implemented, for instance, using bitwise XOR: to encrypt the message \( p \), compute \( c = k \oplus p \); to decrypt \( c \), compute \( p = k \oplus c \).

\[
\text{type block = b:bytes } \{ \text{Length } b = n \}
\]

\[
\text{let encrypt k p = xor k p}
\]

\[
\text{let decrypt k c = xor k c}
\]

Next, we explain how to specify and prove that an encryption scheme is secure. In cryptography, confidentiality is usually stated as resistance against chosen-plaintext attacks (CPA) and encoded as a decisional game in which an adversary chooses two plaintexts, receives the encryption of one of them under a fresh key, and must guess which of the two plaintexts was encrypted. (Decryption plays no role in this simple game: still, we may typecheck that it undoes encryption using classical refinements and properties of XOR.) This game may be coded in RF* as follows:

\[
\text{let cpa b p0 p1 = let p = if b then p0 else p1 in encrypt (sample n) p}
\]

where \( b \) is private and \( p0, p1 \), and the result are public. We thus express (perfect) CPA security relationally with the following type:
val cpa : b : bool → eq block → eq block → eq block

stating that the encryption of one of the two chosen-plaintext blocks
p₀ or p₁ depending on b does not leak any information about b,
hence does not help the adversary to win the game.

In fact, viewing CPA security from an information flow perspec-
tive, a simpler formulation is possible. Instead of reasoning about
two messages selected by b, we just need to show that the function
let cpa' p = encrypt (sample n) p has the type block → eq block.
This is the best type we can hope for encryption, treating the plaintext
as private and the ciphertext as public. This more compact typing
property subsumes the first one.

To prove secrecy for the one-time pad, some probabilistic rea-
soning is called for. Indeed, operationally, calling sample n twice
does not usually return the same value. However, relying on our
formal semantics, we show that it is permissible to give sample a
more specific relational type that allows us to complete the proof.
In particular, as explained below, we can type the call to sample n
in a way that depends on the plaintext p and give it the type
m : block \{ | xor (L p) (L m) = xor (R p) (R m) \}

From this type, RF⁺ automatically proves cpa' : block → eq block.
Intuitively, this relational refinement is sound inasmuch as the dis-
bution of the resulting ciphertext is independent of the plaintext.

In programs that contain sample, the interpretation of assertions
in the RST monad becomes probabilistic. We formalize this in §3,
but provide some intuition for their meaning here. If we can give
the type RST (λ_ _ . True) T to e₀ ~ e₁, then our logic guarantees that
if Q is an equivalence relation partitioning t in a set of equivalence
classes \( \bar{S} \), and if running e₀ in a heap h₀ reduces to e₁ and in
two red states v₁ reduces to v₁, then for any S ∈ \( \bar{S} \), the probability that v₀ ∈ S
is equal to the probability that v₁ ∈ S. Similar conclusions can be
drawn in general. For example, if Q \( \cong \) h₀ h₁ x₀ x₁ h₀' h₁' implies
\( P₀ \times P₁ \Rightarrow P₁ \times x₁ \), then the validity of the above assertion implies that
\( \Pr[\{P₀ \times v₀ \Rightarrow P₁ \times v₁ \}] \).

From this interpretation, one should be able to see that the re-
lational refinement on the result of sample in RF⁺ is not specific to
XOR. More generally, sample can be given a specification to state
that any two calls to it return a pair of values related by any given
one-to-one function on its range. Intuitively, relational refinements
in RF⁺ capture relations between the distribution over values gen-
erated by probabilistic programs, rather than between values obtained
in specific executions. The relational typing of sample is valid since
applying a one-to-one function to a value uniformly chosen from a
discrete set does not change its distribution.

To reflect these general properties of uniform sampling, our
library provides a polymorphic, typed variant of sample, that takes
as additional ghost parameter F, a binary predicate on sampled
values of type block, whose refinement states that F must be an
injective function (or, equivalently, a bijection). This parameter has
kind block → block = E, where E is the kind of ghost refinements
in RF⁺ (types in E are erased at runtime). In the RF⁺ standard library,
sample is typed as follows
type Function F = Ψa.\ Ξb.F a b ∧ Ψa b₁ b₂.F a b₁ ∧ F a b₂ =⇒ b₁ = b₂
type Injective F = Function Ψa.\ Ξa b₁ a₂.F a b₁ ∧ F a b₂ =⇒ a₁ = a₂
val sample : ∀F. len: nat (Injective F) → block len \{ F (L b) (R b) \}

In our one-time pad example, when calling sample n in cpa' , we
instance F to \( \lambda b_0 b_1. \) xor (L p) b₀ = xor (R p) b₁, which is indeed
injective. In §5, we describe security proofs of more realistic en-
cryption schemes based on variants of the above typing for sample.

### 2.4 Implicit flows and passport luminosity

Before justifying our typing rules, notably for sample, we present a concrete pro-
tocol for RFID-equipped passports, implemented in RF⁺, and we
discuss a linkability attack against this protocol recently uncovered

<table>
<thead>
<tr>
<th>Passport Tag</th>
<th>(physically sharing k)</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>sample nt</td>
<td></td>
<td>sample nr, kr</td>
</tr>
<tr>
<td>decrypt</td>
<td></td>
<td>decrypt</td>
</tr>
<tr>
<td>verify MAC</td>
<td></td>
<td>verify MAC</td>
</tr>
<tr>
<td>verify nt</td>
<td></td>
<td>verify nr</td>
</tr>
<tr>
<td>sample kt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>{ nr | nt | kt }k</td>
<td>{ nt | nr | kr }k</td>
<td></td>
</tr>
<tr>
<td>exchange data</td>
<td></td>
<td>s = kt ⊕ kr</td>
</tr>
</tbody>
</table>

![Figure 1. Basic Access Control protocol for passports](image)

by Chothia and Smirnov [19]. They refer to our work for a detailed
discussion. This attack is representative of common weaknesses in
cryptographic implementations due to implicit flows in the han-
dling of errors while processing decrypted data.

Following the ICAO specification for machine-readable travel
documents, all recent European passports embed RFID tags fea-
turing the Basic Access Control protocol, outlined in Fig. 1. The
protocol has two roles, a passport tag and a reader, exchanging mes-
ages using short-distance wireless communications. The goal of
the protocol is to establish a shared session key for accessing bio-
metric data on the passport. Each passport tag has a unique key k,
the reader derives this key from information obtained by scanning
the passport. (In reality, there is a negligible chance of two pass-
ports having the same key, because the key is derived from a hash
of this information.)

The passport first samples a 64-bit nonce nt and sends it as a
challenge to the reader. The reader samples its own nonce nr and
some keying materials kr, then encrypts the concatenation of these
three values using k. Concretely, the protocol implements authen-
ticated encryption as triple-DES encryption concatenated with a
plaintext Message Authentication Code (MAC). The passport de-
crypts, recomputes and checks the MAC to ensure that the message
has not been tampered with, then compares the received nonce nt
with the challenge, to confirm that the reader responded correctly.
If both checks succeed, it generates its own keying materials kt,
appends them to the concatenation of the two nonces (in a different
order than before), and computes the session key s = kt ⊕ kr.
The reader then similarly decrypts the received ciphertext, checks
the MAC, and computes s.

The code the tag uses for handling the encrypted message of the
reader is shown below: encrypt and decrypt provide authenticated
crypting; concat and split convert between triples of 64-bit values
and their concatenation.

let tag1 k nt c = match decrypt k c with
| Some p → let (nt', nr, kr) = split p in
| if nt = nt' then encrypt k (concat nr nt (sample kt))
| else noneError
| None → decryptError

The code either produces an encrypted message, or it returns an
error code. As written, it enables the following linkability attack:

1. The attacker eavesdrops any run of the protocol between a
target passport and an honest reader, and records their second
message.
2. Later, to test the local presence of this passport, the attacker
runs the protocol (as the reader), replays the recorded message,
and observes the response: although the protocol always fails to
establish a key, the tag returns a noneError if the two passports
are the same, and a decryptError otherwise.

Experimentally, French passports reliably return different error
messages, whereas other European passports return the same er-
ror message, but with measurably different timings. Although our approach does not directly catch timing attacks, those attacks can be conservatively analyzed by treating error codes produced at different code locations as distinct.

We interpret the above attack as an implicit flow of information from the key used to decrypt to the error message. Indeed, if we type the key \( k \) as high confidentiality and the nonce \( n \) and the cipher \( c \) with eq refinements (since they are exchanged on a public network), relational typechecking fails on the body of \( \text{tag1} \). The result of the decryption is (a priori) not the same on both sides, so the cross-cases involve proving, for instance that when decryption returns Some \( p \) on the left and None on the right, the two resulting expressions are equal, which fails on the proof obligation \( \text{nonceError = decryptError} \).

By ensuring that the same error messages are returned in both cases (i.e., by requiring that \( \text{nonceError = decryptError} \)) this case is prevented, but this alone is not sufficient for verifying the code. Naively, the cross-cases that arise when verifying the nested conditions require proving, under a suitable relational path condition, that the encryption on the third line is indistinguishable from the error messages—which is patently false. However, by reflecting several cryptographic assumptions into detailed typing invariants in the protocol implementation, we can prove that such problematic cross-cases never actually arise (i.e., the path conditions guarding these cases are infeasible) and we can verify that this code preserves unlinkability. Specifically, we assume that the encryption is CPA, key-hiding, and CTXT (all specified by typing) and that there are no nonce collisions (the probability of a collision is less than \( q^{2−64} \) where \( q \) is the number of sessions observed by the adversary). Arapinis et al. [5] also analyze the corrected protocol, using the applied \( \pi \)-calculus, essentially proving unlinkability in a more abstract, symbolic model of cryptography. Please refer to our online materials for a full listing and further discussion of the specification and implementation of \( \text{tag1} \).

3. Formal development

We formalize a core of \( \lambda F \) in the Coq proof assistant by developing \( \lambda_p \), a minimal higher-order language with (statically allocated) references, probabilistic assignments, and unbounded recursion. The formalization is based on the SSRReflect extension [26], and on the ALEA library for distributions [6]. Overall, the formalization comprises over 2,500 lines of code excluding the aforementioned libraries.

The formalization is built in two steps. First, we consider a simply typed system \( G \vdash e : T \) for \( \lambda_p \). Simple types \( T \) are extended to relational refinement types \( C \) where one can add relational pre- and post-conditions to function types. This allows us to define a relational type system \( G \vdash e_0 \sim e_1 : C \) that relates a pair of expressions \( e_0 \) and \( e_1 \) in the type \( C \) under the relational context \( G \).

We then give a denotational semantics for well-typed judgments. Simple types are given a cpo interpretation \( [T] \) in the standard way. Judgments \( G \vdash e : T \) are interpreted as the elements of the form \( [\psi]_I \), where \( I \) is any valuation for the context \( G \). Taking into account that \( \lambda_p \) is a language with references and probabilistic assignments, the denotation \( [\psi]_I \) of \( e \) is defined as a function from memories (equivalently, states or heaps) to distributions over pairs composed of a memory and an element of \( [T] \); we denote by \( M([T]) \) this function space. Relational types \( C \) are interpreted as a binary relation \( [C] \) over \( M([T]) \), where \( T \) is the simple type derived from \( C \) by erasing all refinements. This allows us to interpret (Theorem 1) a valid judgment \( G \vdash e_0 \sim e_1 : C \) by all the pairs of the form \( ([\psi_1]_{I_L}, [\psi_2]_{I_R}) \in [C] \) for any pair of valuations \( (I_L, I_R) \) for the erasure \( G \) of \( G \).

\[
\begin{align*}
x & : T \in G \quad \tau \in \{L, R\} \\
G \vdash \tau \vdash x & : T \\
G \vdash G' & \quad \text{for} (x : T) \\
r & : \text{ref B} \quad \tau \in \{L, R\} \\
G \vdash \tau \vdash r & : B \\
G \vdash G' & \quad \text{for} (r : B) \\
G \vdash v_1 & : T \quad G \vdash G' \vdash v_1 \vdash v_2 \\
G \vdash G' & \quad \forall \phi : B, \phi \\
G \vdash G' & \quad \forall y : B, \phi \quad \text{for} (y : B)
\end{align*}
\]

Figure 2. Well-formed relational formulas (excerpt)

3.1 \( \lambda_p \): syntax. \( \lambda_p \) is a simply typed \( \lambda \)-calculus with references and probabilistic assignments. For simplicity, we only consider two forms of probabilistic assignments: assigning a uniformly sampled boolean to a boolean variable (flip), and assigning an integer value sampled uniformly in a non-empty interval \([i, j]\) to an integer variable (pick\( j \)). Formally, the sets of types, contexts, values and expressions are given by the following grammars:

\[
\begin{align*}
type & : T :::= B | T \rightarrow T \\
ctx. & : G :::= [] | G, [x : T] \\
value & : v, u :::= c | x | o(v_1, \ldots, v_n) | \text{fun } x : T \rightarrow e \\
expr. & : e :::= v | e \rightarrow e | \text{if } x :::= v \rightarrow \text{flip } \text{pick} j | \text{let } x :::= e_1 \text{ in } e_2 \\
& \quad \text{| letrec } f :::= e_1 \text{ in } e_2 \quad \text{| if } v \text{ then } e_1 \text{ else } e_2 
\end{align*}
\]

where \( x \) ranges over a set of variables, \( r \) ranges over a set of references and \( o \) ranges over a set of \( \text{B} \)-sorted operators, whose signature is of the form \( B_1 \times \cdots \times B_n \rightarrow B_o \). We assume that \( B \) contains the unit type (unit) along with the types of Booleans (bool) and integers (int). Their associated constructors are \( \bullet, \text{true, false} \) and \( n \) for \( n \in \mathbb{N} \). We implicitly assume that each reference has an ambient base type, and write \( r : \text{ref B} \) to denote that \( r \) is a reference with base type \( B \). The dynamic semantics is defined in the standard way as the comparable closure (for a call-by-value convention) of the \( \beta \eta \)-contraction.

3.2 \( \lambda_p \): typing. As usual, a typing context is a sequence of bindings \( x : T \) such that the bound variables are pairwise distinct.

The typing rules for deriving valid judgments \( G \vdash v : T \) and \( G \vdash e : T \), in a simply typed setting, are standard and omitted.

RELATIONAL REFINEMENT TYPES. Relational assertions are formulas over tagged variables \( x_L \) or \( x_R \) and tagged references \( r_L \) or \( r_R \); informally, tags determine whether the interpretation of \( x \) or \( r \) will be taken w.r.t. the left or right projection of a relational valuation. In order to interface with automated first-order provers, relational assertions are first-order \( \text{B} \)-sorted formulas built from operators in \( C \) and predicates taken from a set of \( \text{B} \)-sorted predicates that includes at least the equality predicates for all the base types. Note that tagged variables always occur free in assertions, and only logical variables can be bound. For instance, the relational assertion \( \forall y : \text{int}, x_L \leq y \Rightarrow x_R \leq y + r_R \) is well-formed under any context \( G \) such that \( x : \text{int} \in G \), assuming that \( r : \text{ref int} \).

Formally, relational assertions are defined using a first-order type system with judgments of the form \( G \vdash G' \vdash \Phi \) for formulas (resp. \( G \vdash G' \vdash v : T \) for values) where \( G \) (resp. \( G' \)) is a context for relational variables (resp. for non-relational variables introduced by quantifiers). Figure 2 shows the typing rules for variables, references, equality, and universal quantification. We say that an assertion \( \Phi \) is well-formed in context \( G \) if \( G \vdash \emptyset \vdash \Phi \) (written \( G \vdash \Phi \)).

Refinement types are either relational types (denoted by \( T, U, V \)), which will be used for relational typing of values, or computation types (denoted by \( C \)), used for relational typing of expressions.
They are defined by the following grammar:

\[
T, U, V ::= B \mid (x : T) \to C \quad C ::= \{\Phi\} x : T(V)
\]

where \(\Phi\) and \(\Psi\) are relational assertions. By convention, \(x\) is bound in \((x : T) \to C\) and \(\{\Phi\} x : T(V)\), and can be free in \(C\) or \(\Psi\).

However, the type system enforces that \(x\) occurs in \(C\) and \(\Psi\) only if \(T\) is a base type. In other cases, we write \(T \to C\) and \(\{\Phi\} x : T(V)\).

A relational context \(G\) is a sequence of bindings \(x : T\) such that the bound variables are pairwise distinct. The refinement type \(T\) is a refinement of \(T\) under \(G\), written \(G \vdash T <\to \triangleleft T\), if \(T\) is the result of erasing all pre- and post-conditions occurring in \(T\) and if any assertion \(\Phi\) that appears in \(T\) is well-formed in \(G\) augmented by the local context of \(\Phi\) in \(T\). This relation is extended to relational contexts: \(G \vdash A \triangleleft B\) is the smallest relation such that \([A \triangleleft B]\) if and only if \(G \vdash A \triangleleft B\) and \(G \vdash T <\to \triangleleft T\) then \(G, x : T \vdash A, x : T\).

**Relational Typing.** Figure 3 gives a significant subset of the rules that define the relational typing judgments \(G \vdash v_1 \sim v_2 : T\) for values and \(\{A \triangleleft B\} x : T(V)\) for expressions. In the figure, \(e[x := e_0, e_1] \equiv e[x_L := e_0] [x_R := e_1]\). The full set of rules appear in the accompanying Coq formalization.

A judgment of the form \(G \vdash e_1 \sim e_2 : \{\Phi\} x : T(V)\) is valid when, for any pair of values \(I_L, I_R\) for \(e_i\) and any pair of states \(m_1, m_2\) satisfying the pre-condition \(\Phi\), the distributions over states and values obtained by executing \(e_1\) in \(I_L, m_1\) and \(e_2\) in \(I_R, m_2\) are related by the lifting of the post-condition \(\Psi\) to distributions.

The formal notion of lifting a relation to distributions is given below. We anticipate that although assertions in relational refinements are first-order formulas that do not mention probabilities, the definition of lifting is such that valid typing judgments can be used to prove relations between probability quantities. For instance, when \(\Psi\) denotes an equivalence relation on \(T\), \(\| e_1 \equiv e_2 \equiv \{\text{true}\} x : T(V)\) implies that \(\text{Pr}(e_1 \in S) = \text{Pr}(e_2 \in S)\), for any equivalence class \(S\) of \(\Psi\). Intuitively, observing to which equivalence class the results belong does not help in distinguishing the two expressions. As sketched in §2.3, we are not limited to simply proving probabilistic equivalences; other kinds of probabilistic assertions (e.g., inequalities) can also be expressed.

The rules come in two flavors: double-sided or single-sided. Double-sided rules allow us to relate programs with the same head symbol. For instance, rules \([\text{Let}]\) and \([\text{Aref}]\) are double-sided. They work by relating sub-expressions pairwise, composing pre- and post-conditions using the implicit order of evaluation. Rule \([\text{Let}]\) emphasizes this, with the post-condition of the let-bound expression being the pre-condition of the body.

It is not always possible to progress using double-sided rules. For instance, one may want to show that the two expressions \((f\ b\ \text{then}\ v\ \text{else}\ v)\) and \(v\) are related by a suitable post-condition. The two expressions having different head symbol, no double-sided rule can apply. Single-sided rules allow us to overcome this limitation. Rule \([\text{Let-Left}]\), which permits to relate an if-expression to an arbitrary expression, is an example of a single-sided rule.

All the single-sided rules come in pairs: one variant (tagged \([\text{Let-Left}]\)) where the progression is done on the left expression, and one (tagged \([\text{Let-Right}]\)) where the progression is on the right. Instead of showing both cases explicitly, we give a general rule \([\text{Sym}]\) that transforms any \([\text{Let-Left}]\) rule into its \([\text{Let-Right}]\) counterpart.

Rules for reference assignment \((\text{[Ref]}\), \([\text{Ref-Left]}\), which come in two flavors too, make use of the ability to write assertions about the resulting memory. For example, the two expressions \(r := v_0\) and \(r := v_1\) are related by a post-condition \(\Psi\) when \(\Psi\), after replacing all occurrences of \(r\) (resp. \(r_\Psi\)) with \(v_0\) (resp. \(v_1\)), holds as a pre-condition.

So far, we only considered rules for expressions headed by non-probabilistic constructions. Rules for random sampling \(([\text{Flt}]\) and \([\text{Sample}]\) are double-sided and require the existence of a bijection \(f\) between the support of the two distributions, ensuring a one-to-one correspondence between related values. In the case of \([\text{Flt}]\), we explicitly give the only two existing bijections from \text{bool} to \text{bool}.

### 3.3 λP: denotational semantics.

**Background.** The denotational semantics of well-typed expressions is based on the sub-probability monad over sets [6, 37] and its generalization to complete partial orders (cpos); recall that a cpo is a partial order in which every ascending chain has a supremum.

The unit interval \([0, 1]\) has a cpo structure w.r.t. the natural order on reals; moreover, every set can be lifted to a flat cpo by adding a bottom element, and the set of functions \(A \to B\) between a set \(A\) and a cpo \(B\) can be given the structure of a cpo. A function between two cpos is monotonic if it is order-preserving, and it is continuous if it is monotonic and preserves suprema. Given two cpos \(A\) and \(B\), we let \(A :\!\!\!\to B\) and \(A \to B\) denote the set of monotonic and continuous functions from \(A\) to \(B\) respectively. By Kleene’s fixed point theorem, every continuous function \(f\) on a cpo has a least fixed point \(\text{fix}\ f\).

A discrete sub-distribution over a set \(X\) is a continuous functional \(\mu: (X \to [0, 1]) \to [0, 1]\) that satisfies axioms of linearity, compatibility with inverse, and discreteness. In particular, the latter axiom states that the support \(\text{supp}(\mu)\) of \(\mu\), consisting of all elements \(x \in X\) such that \(\mu(x) > 0\), is discrete—where \(\delta_x\) denotes the Dirac function for \(x\): i.e., \(\delta_x(y) = 1\) if \(x = y\). We let \(D(X)\) be the set of discrete sub-distributions over \(X\).\(D(X)\) has the structure of an \(\omega\)-complete partial order. Moreover, sub-distributions can be given the structure of a monad; the unit and composition operators are denoted by \(\text{unit}\) and \(\text{bind}\) respectively.

The relational interpretation of types rests on an operator \(\text{lift}\) that lifts relations over \(A \times B\) into relations over \(D(A) \times D(B)\); the operator is inspired from early works on probabilistic bisimulations [28], and is used in CertiCrypt [7] and EasyCrypt [9] to interpret relational judgments. Formally, let \(\mu_1 \in D(A)\) and \(\mu_2 \in D(B)\); then \(\text{lift} [\mu_1 \mu_2] \text{iff}\):

\[
\exists \mu : (A \times B). \pi_1(\mu) = \mu_1 \land \pi_2(\mu) = \mu_2 \land \text{supp}(\mu) \subseteq R
\]

where \(\pi_1\) and \(\pi_2\) are the projections for distributions over pairs, i.e.,

\[
\begin{align*}
\pi_1(\mu) &= \text{bind } \mu (\lambda (x, y). \text{unit}\ x) \\
\pi_2(\mu) &= \text{bind } \mu (\lambda (x, y). \text{unit}\ y)
\end{align*}
\]

A fundamental property of this lifting operator is that given \(f: A \to [0, 1]\) and \(g : B \to [0, 1]\) such that \(\forall a \in A, b \in B. \text{ref } a = b = f a = g b\)

then \(\text{lift} [\mu_1 \mu_2] \text{implies that } \mu_1 f = \mu_2 g\), i.e., the expected values of \(f\) in \(\mu_1\) and \(g\) in \(\mu_2\) coincide. Note that events can be viewed as \([0, 1]\)-valued functions, and in this case expectation coincides with probability.

**Interpretation.** We first provide a non-relational interpretation of valid judgments. We assume each base type \(B\) is interpreted as a (flat) cpo \([B]\), and that each constructor \(c\) belonging to the base type \(B\) is given a denotation \(B(c) \in \{B\}\). We define the set of semantical values as \(\Pi_{[B]}\), and then the set \(M\) of \text{states} as the set of well-typed mappings from references to semantical values.

\[
M = \{m : \text{ref} \to \Pi_{[B]} \mid \forall r : \text{ref} B. m(r) \in [B]\}\]

Then we extend the interpretation to functional types by setting

\[
\text{M}(f) \equiv M \to D(X \times M)
\]

A valuation \(I\) is a function that maps every declaration \(x : T\) to a semantical value. A valuation \(I\) is well-formed for \(G\), written \(I \vdash G\), if \(I\) maps every declaration \(x : T\) in \(G\) to an element of \([T]\).
Let $I$ be a valuation and $m$ be a memory. The interpretations \([v]_I\) of a value $v$ and \([\Phi]^I\) of an expression $\Phi$ are defined in Figure 4. If $I$ is a well-formed valuation for $G$, and $G \vdash v : T$ is derivable, then \([v]_I \in [T]$. Likewise, if $G \vdash e : T$ is derivable then $\lambda m. [e]^I \in M([T])$.

We now turn to giving a relational interpretation of valid judgments. A well-formed relational valuation $\I$ for $G$, written $\I \vdash \Psi$, is a pair of well-formed valuations for $G$. If $\I = (I_1, I_2)$, we write $\pi_1(\I)$ (resp. $\pi_2(\I)$) for $I_2$ (resp. $I_1$), and $\I(x)$ for $(I_1(x), I_2(x))$. We assume given a relational interpretation for formulas, written $[\Psi]_\I$, such that for any formula $\Phi$ well-formed under $G$, for any relation valuation $\I \vdash \Phi$, $[\Phi]_\I$ is a binary relation on $M$. This relation is defined as usual, using the left/right valuation (resp. left/right memory argument) for interpreting variables on the left/right (resp. references on the left/right). Figure 5 defines the interpretation of relational types, written $[\Phi]_\I \subseteq \T$, and computation types, written $[\Phi]_\I \subseteq \C$, w.r.t. a relational valuation $\I$. A relational valuation $\I$ is well-formed w.r.t a relational context $\G$, written $\I \vdash \G$, if for any context $\G$ such that $\G \circ \G$, and every variable $x$ declared in $G$, $\I(x) \in \langle \I \vdash \I \circ \G(x) \rangle$.

Finally, we define the semantic validity of judgments: we say that two values $v_1$ and $v_2$ are semantically related in $\T$ under $\G$, written $\I \vdash v_1 \sim v_2 : \T$, if $\G \circ \G$, and $\I \vdash \T \sim \T$, and

\[
\forall \T \vdash \G, \forall v_1, v_2 : \T \Rightarrow \langle \I \vdash \I \circ \G(x) \rangle.
\]

We say that two expressions $e_1$ and $e_2$ are semantically related in $\C$ under $\G$, written $\I \vdash e_1 \sim e_2 : \C$, if $\G \circ \G$, and $\I \vdash \C \sim \C$, and

\[
\forall \C \vdash \G, \forall e_1, e_2 : \C \Rightarrow \langle \I \vdash \I \circ \G(x) \rangle.
\]

The following theorem states that all judgments of the logic are sound w.r.t. their interpretation; it implies that typing can be used to verify probabilistic claims, thanks to the properties of lifting.

**Theorem 1.** (Soundness). Let $\G \vdash v_1 \sim v_2 : \T$, then $\I \vdash v_1 \sim v_2 : \T$, and

- If $\I \vdash e_1 \sim e_2 : \C$, then $\I \vdash e_1 \sim e_2 : \C$.

\[
\begin{align*}
\end{align*}
\]
4. Encoding $\lambda_p$ in RF

We now discuss our language design and implementation. There are two key ideas behind our encoding of $\lambda_p$ in RF. First, as shown in §2.3, we introduce probabilistic computations into $F^*$ axiomatically, by providing a sample primitive at the appropriate type. Programmers can instantiate sample at runtime by providing a suitable source of randomness. Next, as discussed in §2.2, we adapt the Hoare-style monad $ST$ to a monad $RST$ for computations with relational pre- and post-conditions. We provide here more details about our encodings, in particular the style we adopt to compute relational verification conditions for the $RST$ monad, and the manner in which we reuse classical specifications.

4.1 Representing $\lambda_p$ types. To implement $\lambda_p$, we begin with a translation of its types into $F^*$ augmented with a relational state monad. To stay close to $\lambda_p$, our translation uses a monad $RST_0$, which we then adapt to the monad $RST$ of §2. Like in $\lambda_p$, post-conditions in $RST_0$ only relate the output values and heaps, not the initial heaps. Specifically, the type $RST_0 \alpha \beta \preceq \sigma \tau$ can be interpreted in $F^*$ as a step-function passing a (primitive heap) with the signature shown below:

$$\text{RST}_0 \alpha \beta \preceq \sigma \tau \Rightarrow \text{hp} \cdot \text{heap } \{ \text{post } (L, h) \} \Rightarrow (x : \text{hp} \cdot \text{heap } \{ \text{post } (L, h) \} (L h') \Rightarrow (R h) \} \}$$

The type translation is homomorphic on most of $\lambda_p$’s typing constructs, with the interesting cases mainly on the computation types, where $[\Phi y : T \cdot \{ \Psi \}]$ is $\text{RST}_0 \Phi [\Psi y : T \cdot \{ \Psi \}]$.

4.2 A monad of predicate transformers for VC generation. Next, to provide type inference for $RST_0$, rather than writing relational Hoare triples in $RST_0$, we write specifications using predicate transformers. This style is adapted from the Dijkstra state monad, previously introduced for inferring classical (non-relational) verification conditions for stateful F programs [46]. In particular, we introduce the relational Dijkstra state monad, $RSTD$, and show its signature below. (We write polymorphic types implicitly assuming their free type variables are quantified beforehand.)

$$\text{RST}_0 \preceq \text{post } \Rightarrow \text{hp} \cdot \text{heap } \{ \text{post } (L, h) \} \Rightarrow (x : \text{hp} \cdot \text{heap } \{ \text{post } (L, h) \} (L h') \Rightarrow (R h') \} \}$$

The type $RSTD \alpha \beta \preceq \sigma \tau$ is an abbreviation for the $RST_0$ monad that is polymorphic in its post-condition. Specifically, $RSTD \alpha \beta \preceq \sigma \tau$ is the type of computation which for any relational post-condition $\alpha$ on $\text{ts}$ and $\text{heaps}$, the pre-condition on the input heaps is given by $wp_\beta$.

Unlike the Hoare-style $RST_0$ monad, the $RSTD$ monad yields a weakest precondition calculus by construction. As indicated by the signature of bind, when composing computations in the $RSTD$ monad, we simply compute a pre-condition for the computation by composing the predicate transformers of each component. A slight complication arises from the need to constrain the formal parameter $\text{x:a}$ of $wp_\beta$ relationally. In general, $wp_\beta$ will have free occurrences of $L x$ and $R x$. We relate these to the result of the first computation using the guard $L x = 0$ and $R x = 1$, before composing $wp_\alpha$ and $wp_\beta$. Additionally, by exploiting the post-condition parametricity of $RSTD$, we can recover the expressiveness of a 6-place post-condition relation in the $RST$ monad that we use in our examples. We show the definition of $RSTD$ below.

\[
\text{type } \text{RST}_0 \preceq \text{post } \Rightarrow \text{RST}_0 \alpha \beta \preceq \sigma \tau \Rightarrow \text{RSTD } \alpha \beta \preceq \sigma \tau \Rightarrow \text{RSTD } \alpha \beta \preceq \sigma \tau \Rightarrow \text{RSTD } \alpha \beta \preceq \sigma \tau \Rightarrow \text{RSTD } \alpha \beta \preceq \sigma \tau \Rightarrow \text{RSTD } \alpha \beta \preceq \sigma \tau
\]

4.3 Lifting classical specifications. To promote reuse of existing verified $F^*$ code in RF, we provide combinators to lift specifications written with classical predicate transformers into the $RSTD$ monad. To illustrate our approach, we show the $RF^*$ specifications of primitive operations on references—the same combinators apply to arbitrary classically verified code.

\[
\text{type } \text{lift wp}_0 wp_1 \alpha \beta \preceq \sigma \tau \Rightarrow \text{RSTD } \alpha \beta \preceq \sigma \tau
\]

The combinator lifts two classical predicate transformers $wp_0$ and $wp_1$ and composes them by, in effect, “running” them separately on the heaps $h_0$ and $h_1$ and relating the results and heaps using the relational post-condition $\preceq$. The types given to dereference and assignment should be evident—these are simply the relational liftings of the standard, classical weakest pre-condition rules for these constructs ($\text{Rd}$ and $\text{W}$, respectively).

4.4 Computing relational VCs. We re-purpose the bulk of $F^*$’s type-checking algorithm to RF. Although the relational typing rules of Fig. 3 generally analyze a pair of programs $e_0 \sim e_1$, for the most part, we are concerned with proving relational properties of multiple executions of a single program. Thus, in the special symmetric case where we are analyzing $e \sim e$, the two-sided rules of Fig. 3 degenerate into the standard typing rules for monadic $F^*$ (which is parametric in the choice of monad, so configuring it to use $RSTD$ is easy).

The main subtlety in computing relational VCs arises when analyzing the cross-cases of conditional expressions—for this we implement the single-sided rules in the judgment, and we attempt to revert to the symmetric case as soon as we detect that the program fragments are indeed the same. For example, the rule $[\text{if}]$ allows us to relate if $b$ then $e$ else $e'$ in $e$, by generating subgoals for $e \sim e$ and $e' \sim e$, where at least the former can be handled once again by the symmetric rules.

The rules $[\text{Red-Left}]$ and $[\text{Red-Right}]$ of Fig. 3 are impossible to implement in full generality—they permit reasoning about stateful programs after arbitrary reductions of open terms. Instead, these rules are approximated by the $RF^*$ typechecker for terms that can be given classical predicate transformer specifications. In particular, when trying to relate $e_0 \sim e_1$, if we can use the symmetric judgments and type $e_0 \sim e_0 : \text{RSTD } t (\text{lift wp}_0)$, and $e_1 \sim e_1 : \text{RSTD } t (\text{lift wp}_1)$, then we type $e_0 \sim e_1$ at type
\[
\begin{align*}
&f_1, f_2 \in [\mathbb{T}] \rightarrow \mathcal{M} \rightarrow D(\{\mathbb{U}\} \times \mathcal{M}) \\
&\forall t_1, t_2 \in \{G \vdash T \triangleleft \mathbb{T}\}_x, (f_1, t_1, f_2, t_2) \in \{G \vdash C \triangleleft \mathbb{U}\}_{I[x=(t_1, t_2)]} \\
&(f_1, f_2) \in \{G \vdash (x : \mathbb{T}) \rightarrow C \triangleleft \mathbb{T} \rightarrow \mathbb{U}\}_x \\
&(d_1, d_2) \in \{\mathbb{B}\}^2 \\
&(d_1, d_2) \in \{G \vdash B \triangleleft \mathbb{B}\}_x \\
&\forall m_1, m_2 \in \mathcal{M}, \{\Psi\}_{x=(m_1, m_2)} \vdash \{\Phi\}_{y=(u_1, u_2)} \vdash T \\
&\forall \mu_1, \mu_2 \in \mathcal{M} \\
&\mu_1, \mu_2 \in \{G \vdash T \triangleleft \mathbb{F}\}_x \\
&\{\mu_1, \mu_2\} \in \{G \vdash (\forall \cdot y) : U(\Psi) \triangleleft \mathbb{U}\}_x \\
&\mu = \lambda((u_1, m_1'), (u_2, m_2')). (u_1, u_2) \in \{G \vdash U \triangleleft \mathbb{U}\}_x \wedge \{\Psi\}_{x=(u_1, u_2)}(m_1', m_2') \\
\end{align*}
\]

\begin{table}[h]
\centering
\begin{tabular}{|c|c|}
\hline
$P$ & $= \lambda((u_1, m_1'), (u_2, m_2')). (u_1, u_2) \in \{G \vdash U \triangleleft \mathbb{U}\}_x \wedge \{\Psi\}_{x=(u_1, u_2)}(m_1', m_2')$
\hline
\end{tabular}
\caption{Interpretation of relational refinement types}
\end{table}

RDST t (lift wp0 wp1). In effect, by making use of classical predicate transformers on either side, we approximate the reduction relation for stateful terms used by \texttt{RED-LEFT} and \texttt{RED-RIGHT}.

All these measures for handling the asymmetric cases are still incomplete. When trying to prove a relation between $f v_1 \sim g v_1$ in a context $G$ with relational types for $f$ and $g$ that cannot be decomposed into a pair of classical specifications, it becomes impossible to complete the derivation. In such cases, RF$^*$ emits \texttt{False} as the VC (guarded by a relational path condition). Nevertheless, it may still be possible to discharge the VC, if the path condition is infeasible. This is the case, for example, when trying to relate the result of encrypt with \texttt{errorNonce} in the passport example of §2.4.

\section{5. Applications}

Table 5 summarizes our experimental evaluation of RF$^*$. For each program, we give the Makefile target name in the F$^*$ distribution, the number of lines of code and type annotations (excluding comments), and the typechecking time in seconds, which is mostly dominated by the time spent solving VCs in Z3. All experiments were conducted on a 3GHz HP Z820 32-core workstation with 32GB of RAM (although the verifier makes use of only one core). For lack of space, most of these examples are only briefly described, with a more detailed discussion of the last two programs, counter in §5.1 (a cryptographic construction) and meter in §5.2 (a privacy protocol).

\textbf{Information flow.} The first five programs provide many information flow examples, such as those of §2.2, and test cases for single-sided rules using several variations of the RDST monad construction of §4.

\textbf{Passport unlinkability.} The sixth program, passport illustrates the verification of the Basic Access Control protocol for RFID-equipped passports, presented in §2.4. It establishes passport unlinkability for the modified protocol that returns the same error message in all failure cases. (As can be expected, the original protocol yields a typechecking error.) Its verification illustrates the use of single-sided rules for nested tests (see tag) in §2.4 and also involves modelling key-hiding symmetric encryption.

\textbf{Random oracles.} The program ro provides an idealized implementation of a cryptographic hash function in the random oracle model. In this model, widely used in applied cryptography, the hash function is assumed to be indistinguishable from a uniformly random function. Thus, knowledge of the hash function values on a subset of its domain yields no \textit{a priori} information about its values outside this subset, and protocols that share the hash function with an adversary can treat those values as secret as long as they use disjoint subsets of its domain. The purpose of ro is to capture this reasoning pattern in a library that enables type-based verification of protocols in the random oracle model.

Our implementation lazily samples (and memoizes) the random function, using a mutable reference holding a table mapping hash queries made by both honest participants $H$ and adversaries $A$. To verify the program, this table carries several invariants, including that the tables grow monotonically; that in every pair of executions, the tables agree on the fragments corresponding to queries made by $A$ and that on the fragments corresponding to queries by $H$, the sampled entries are related by an injective function that ensures they have indistinguishable distributions. The interface of ro is designed to allow the full use of relational sample on the $H$ fragment, and to account for failure events (e.g., returning a value to $A$ that collides with one that was already provided to $H$), allowing for its modular use in a context that must bound their probability.

\textbf{CC2A encryption.} Resistance to adaptive chosen-plaintext and chosen-ciphertext attacks (CC2A) is a standard cryptographic security assumption for public key encryption schemes. To verify protocols relying on this assumption, we program an ideal, stateful functionality for CC2A encryption that maintains a log of prior oracle encryptions, similar to those proposed by Fournet et al. [24], but with a more convenient relational interface. Using the F7 type system with only classic refinements, they require that all code that operates on secrets be placed in a separate module that exports plaintexts as an abstract type. Using instead relational types for secrets, in the style of §2.3, we lift this restriction, enabling us to verify protocol code that uses encryption without restructuring. Our code is essentially higher-order; it simulates ML functions using a dependently typed record of functions.

\textbf{Nonce-based authentication.} Exploiting the modularity of our CC2A implementation, we program and verify simplenonce, a protocol that illustrates a common authentication pattern based on fresh random values, or nonces, formalizing the intuition that, if $A$ encrypts a fresh nonce using the public key of $B$, and later decrypts a response containing that nonce, then the whole response must have been sent by $B$.

\textbf{Private authentication.} Further extending simplenonce, and relying on a key-hiding variant of CC2A, we implement a protocol for private authentication, proposed by Abadi and Fournet [1], that allows two parties to authenticate one another and to initiate private communications without disclosing their presence and identities to third parties. Although the protocol has been studied symbolically in the applied pi calculus, to our knowledge we provide its first verification in a computational model of cryptography.

\textbf{Elgamal encryption.} The chosen-plaintext security (CPA) of ElGamal encryption by reduction to the decisional Diffie-Hellman assumption is a classic example of cryptographic proof. We verify it in RF$^*$, building on an axiomatic theory of cyclic groups.

\textbf{Security “Up to Bad”}. The program uptobad illustrates a common pattern to prove refinement formulas of the form $\varphi \Rightarrow \text{Bad}$ where $\varphi$ is the property we are interested in and \texttt{Bad} captures conditions that may cause the program to ‘fail’, usually with a small probability (e.g. when the adversary guesses a private key). To
avoid polluting all our specifications with this disjunction, we define an up-to-bad variant of the ROST monad, where all pre- and post-conditions, and all heap invariants, are enforced only as long as a distinguished boolean memory reference is false. Intuitively, this adds an implicit ‘∨ Bad’ to every refinement.

Our encoding proceeds in two steps. First, we define msref a p, the type of monotonic references r to an a-value whose contents can be updated only when the update condition p holds. That is, when p is a reflexive transitive binary a-predicate, given two heaps h and h’, if h’ is a successor of h then p(Sel h r) (Sel h’ r) holds. We give below the resulting specification for mwrite, requiring the update condition p as a pre-condition.

<table>
<thead>
<tr>
<th>NAME</th>
<th>LoC</th>
<th>TC(S)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>arith</td>
<td>43</td>
<td>1.5</td>
<td>Information flow with arithmetic</td>
</tr>
<tr>
<td>pure1</td>
<td>35</td>
<td>1.7</td>
<td>Information flow &amp; inference</td>
</tr>
<tr>
<td>pure2</td>
<td>33</td>
<td>1.7</td>
<td>Information flow &amp; inference (variant)</td>
</tr>
<tr>
<td>st</td>
<td>52</td>
<td>3.6</td>
<td>Information flow with state</td>
</tr>
<tr>
<td>single sided</td>
<td>111</td>
<td>14.2</td>
<td>Information flow using single-sided rules</td>
</tr>
<tr>
<td>passport</td>
<td>97</td>
<td>44.2</td>
<td>Unlinkability for RFID passport protocol</td>
</tr>
<tr>
<td>cca2</td>
<td>88</td>
<td>6.5</td>
<td>Idealized CCA2 encryption</td>
</tr>
<tr>
<td>simplicity</td>
<td>108</td>
<td>42.5</td>
<td>Nonce-Based Authentication protocol</td>
</tr>
<tr>
<td>private auth</td>
<td>175</td>
<td>81.4</td>
<td>Private authentication protocol</td>
</tr>
<tr>
<td>elg</td>
<td>217</td>
<td>124.5</td>
<td>ElGamal encryption</td>
</tr>
<tr>
<td>uptobad</td>
<td>106</td>
<td>24.1</td>
<td>Counter mode encryptions using AES</td>
</tr>
<tr>
<td>meter</td>
<td>182</td>
<td>79.8</td>
<td>Commitments &amp; smart meter protocol</td>
</tr>
<tr>
<td>Total</td>
<td>1,378</td>
<td>451.3</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Summary of experiments

5.1 Pseudo-random functions and counter-mode. Resuming from the one-time pad example (§2.3), we implement a more useful symmetric encryption scheme based on a block cipher, such as triple-DES or AES. Blocks are just fixed-sized byte arrays, e.g. 16 bytes for AES. Block ciphers take a key and a plaintext block, and produce a ciphertext block. A common cryptographic security assumption is that the block cipher is a pseudo-random function (PRF): for a fixed key, generated uniformly at random, and used only as input to the cipher, the cipher is computationally indistinguishable from a uniformly random function from blocks to blocks. We first present our sample scheme, then formalize the pseudo-random assumption, and finally explain how we verify it by relational typing.

ENCRIPTING IN COUNTER MODE. The purpose of symmetric encryption modes is to apply the block cipher keyed with a single secret key to encrypt many blocks of plaintexts. In counter mode, to encrypt a sequence of plaintext blocks pi, we use a sequence of index blocks li, obtained for instance by incrementing a counter. We independently apply the block cipher to each li to obtain a mask mi; and compute the ciphertext block ci as pi ⊕ mi, effectively using the masks as one-time pads. A practical advantage of this construction is that both encryption and decryption are fully parallelizable, and that the sequence of masks can be pre-computed. The blocks i need not be secret, but they must be pairwise-distinct. Otherwise, from the two ciphertexts p ⊕ m and p’ ⊕ m, one trivially obtains p ⊕ p’, which leaks a full block of information.

For simplicity, we keep the block cipher key implicit, writing f for the resulting pseudo-random function; we focus on the functions for processing individual plaintext blocks, rather than lists of blocks; and we attach the (public) index to every ciphertext block. First, assume there is a single encrypt, that counts using an integer reference and uses toBytes to format the integer as a block.

let n = ref 0;
let encrypt (p:block) = let i = toBytes l n in n := l + 1; (i, xor f i p)
let decrypt c i c = xor f i c

To enable independent encryptions of plaintext blocks, we can remove the global counter and instead sample a block i for each encryption. As follows, this random block i is called the initialization vector (IV) for the encryption.

let encrypt‘(p:block) = let i = sample 16 in (i, xor f i p)

Much as for the one-time pad, we show that encrypt and encrypt’ can be typed as block → eq (block × block), the type of functions from (private) blocks to pairs of public blocks, under suitable cryptographic assumptions. More general combinations of sampling and incrementing can also be used for independent multi-block encryptions; for instance, the usual counter mode is programmed as:

let encrypt_counter_mode (ps:List block) = let iv = sample 16 in let i = ref iv in iv::List.map (fun p → incrBytes i; xor f i p) ps

PSEUDO-RANDOM FUNCTIONS. To study the security of protocols using a block cipher, we program and type it as a random function from blocks to blocks. (To test our encryption, we also implement it concretely by just calling AES.) If we can prove the security of a protocol using this ideal random-function implementation, then the same protocol using the concrete block cipher is also secure under the pseudo-random-function assumption (with a probability loss bounded by the probability of distinguishing between the two ciphers). We implement the function f using lazy sampling: when called, f first looks up for a previously-sampled mask in its log; otherwise, f samples a fresh mask. As for the one-time pad, we pass the plaintext block p as a ghost parameter, and take advantage of sampling to generate a mask with a relational refinement to specifically hide p. Of course, this fails if the mask has already been sampled, so we type f for encryption with a pre-condition that depends on the current log and requires that i does not occur in the log yet. (We use the same code with a different type for decryption, requesting that i occurs in the log.)

val f : i:Index → p:Block → i:RST pre block post

where

pre p:Block = (∗ Requires: i not in the log yet ∗)
not (ln i (L i) (Domain (Sel h0 (L logi))))
∧ (L i = R i) ∧ (Seq i (L i) < Sel h0 (L n))
and post h0 h1 m0 m1 h0* h1* = (∗ Ensures: log extended with (i,p,m))
Mask (L p) (R p) m0 m1 (∗ and sampling in n’s related by injectivity ∗)
∧ h0* = Upd h0 (L logi) (((Entry i (L i) m0):Sel h0 (L logi))
∧ h1* = Upd h1 (R i (R p) m1):Sel h1 (R logi))
let f p i = match assoc i with
| Some(_,m) → m (∗ unreachable ∗)
| None → let m = sample p in
log := (Entry i p m):!log; m
When using a single counter (function encrypt), typechecking relies on a joint invariant on the counter n and the content of the log that states that all entries in the log have an index block i formatted from some n &lt; n. It also involves excluding counter overflows and assuming that toBytes is injective. This enables us to prove that our encryption is secure with no loss in the reduction: the advantage of a CPA adversary against our code is the same as the advantage of some adversary against the PRF assumption.

When using instead a fresh random block (function encrypt), the situation is more complex, as there is a non-null probability that different encryptions sample the same index i. Our construction is secure as long as no such collisions happen. We capture this event using the "up to bad" approach presented above, for a Fresh module that silently detects collisions and sets the bad flag accordingly. Concretely, the probability of having a collision when sampling q blocks of 16 bytes each is bounded by $q^2/2^{28}$. By typing, we prove that encryption, and any program that may use it, leaks information only once bad is true. Thus, we prove the concrete security of encrypt' with a loss of $q^2/2^{28}$ in the reduction to PRF.

5.2 Privacy-preserving smart metering & billing. We finally implement and verify the "fast billing" protocol of Rial and Danezis [40], which involves recursive data structures and homomorphic commitments. The protocol has three roles:

- a certified meter that issues private, signed, fine-grained electricity readings (say one reading every 10 minutes);
- a utility company that issues public, signed rates (for the same time intervals, depending on some public policy); and
- a user, who receives both inputs at the end of the month to compute (and presumably pay) his electricity bill.

The two security goals of the protocol are to guarantee (1) integrity of the monthly fee paid to the utility company; and (2) privacy of the detailed readings, which otherwise leak much information on the user's lifestyle. The protocol relies on Pedersen commitments [36] and public-key signatures. Next, we explain how we prove perfect, information-theoretic privacy (entirely by relational typing) and computational integrity by reduction to the discrete log problem (by typing using "up-to-bad").

HOMOMORPHIC PEDERSEN COMMITMENTS. We first implement typed commitments, parameterized by some multiplicative group of prime order p. We outline their interface and review their main security properties.

```
type pparams = eq public_param
type opening (pp:pparams) (t:tx) = o:opening (Eq (int (L pp) + t x + L o) (int (R pp) + R x + R o))

val sample: pp:pparams -> t:tx -> opening pp t
val commit: pp:pparams -> t:tx -> opening pp t

let commit pp t r = pp p x + pp x + pp h * r

let verify pp t r c = (c = pp p x + pp h * r)
```

The public parameters pp consists of the prime p and two distinct group generators g and h (possibly chosen by the utility). Texts and openings range over integers modulo p. A commitment to t with opening o is a group element $c = g^h^o$. Although assumed hard to compute, there exists o (known as the trapdoor for these parameters) such that $g = h^o$. Accordingly, we use o as $trap_pp$ for specification purposes, in refinement formulas but not in the protocol code. We use o in particular to specify an injective function for randomly sampling the opening o (modulo p) so that it perfectly hides x: the relational refinement type opening in the post-condition of sample records that $\alpha x = ((L x) + (L o)) = \alpha x (R x) + (R o)$, which implies $g^{\alpha(L x)}h^{\alpha(L o)} = g^{\alpha(R x)}h^{\alpha(R o)}$ and enables us to type the result of commit as public (eq elt). Intuitively, every commitment can be opened to any $x'$, for some hard-to-compute $o'$, so the commitment itself does not leak any information about x as long as o is randomly sampled and kept secret. At the same time, given x and o, it is computationally hard to open the commitment to any $x' \neq x$.

Commitments can be multiplied: $g^{o h^o} = g^{o' h'^o}$ and exponentiated: $(g^{h^o})^p = g^{h^{op}}$ to compute commitments to linear combinations of their exponents without necessarily knowing them. These operations are used below to compute the bill: their (omitted) types show that they preserve eq and opening relational refinements.

Next, we show some typed code for each role of the protocol.

METER. We have abstract predicates Readings and Rates to specify authentic lists of readings and rates. We rely on a signature scheme to sign a list of commitments to private readings; this scheme is assumed resistant against existential forgery attacks; as explained in [24], we express this property using (non-relational) refinements. For simplicity, we keep using and verification keys implicit.

```
type Signed (pp:pparams) (cs:cs) =

\exists xs. Readings (int list elt) \land \land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\land\lang...
6. Related work and conclusions

Our work spans semantics of higher-order probabilistic programs, relational program verification, and cryptographic protocol verification, enabling us to verify the security of protocol implementations under computational assumptions by relational typing.

**Reasoning about Probabilistic Programs.** The semantics of $F^*$ is based on the monadic representation of probabilities used in [6, 37]. Our semantics is confined to discrete sub-distributions; for some applications, such as robotics and machine learning, it is however essential to support continuous distributions. Higher-order programs over continuous distributions are considered in [15, 35].

An alternative approach is to embed probabilistic programming in a general purpose language, as done e.g. by Kiselyov and Shan [29].

Reif [38], Kozen [30], and Feldman and Harel [23] were among the first to develop logics for reasoning about probabilistic programs. Similar logics were later developed by McIver and Morgan [33] and more recently by Chadha et al. [17]. Hurd [27] provides a formalization of the framework of McIver and Morgan in the HOL proof assistant. All these logics are non-relational, and do not allow directly proving relations between probabilities.

**Relational Program Verification.** Relational Hoare Logic was first introduced for a core imperative program to reason about the correctness of program optimizations and information flow properties [11]. It was later extended to probabilistic procedural programs with adversarial code, and used to formally verify reductionist security proofs of cryptographic constructions [7] and differential privacy of randomized algorithms [10]. Relational Hoare Type Theory (RHTT) is an extension of Hoare Type Theory, used to reason interactively about advanced information flow policies of higher-order stateful programs with real world data structures [42]; RHTT does not consider probabilistic computations, which are essential to reason about cryptographic protocols. RHTT is fully formalized as a shallow embedding in the Coq proof assistant. The formalization is restricted to programs with first-order store; but in principle it could be extended to programs with higher-order store using an axiomatic extension of Coq [44]. In contrast, we formalize in Coq a core fragment of $F^*$, and rest on the $F^*$ infrastructure to verify large programs. Our formalization is restricted to programs with first-order store; as we adopt a deep embedding, our formalization could in principle be extended to higher-order store using recent developments in step-indexed semantics [4]. Beyond RHTT and HTT, there have been many efforts to develop and sometimes machine-check program logics for higher-order stateful programs; see [39] for an account of the field.

Relational logics can also be used to reason about continuity [18]. Naturally, numerous program analyses and specialized relational logics enforce 2-properties of programs.

**Comparison with EasyCrypt.** EasyCrypt [8] is a framework for proving the security of cryptographic constructions in the computational model. The core of EasyCrypt is a probabilistic Relational Hoare Logic (pRHL) that is able to capture common patterns of reasoning in cryptographic proofs, including observational equivalence, equivalence up to failure, and reductionist arguments.

The relational refinement type system of $F^*$ is inspired from pRHL, but it also incorporates concerns of compatibility with $F^*$ and automation. In contrast to EasyCrypt, $F^*$ offers only limited support to carry relational reasoning about structurally different programs, and to reason about probabilities of postconditions—the latter is achieved in EasyCrypt using a probabilistic (but non-relational) Hoare Logic, which has no counterpart in $F^*$. As a consequence, some cryptographic constructions whose formalization in EasyCrypt requires interactive game-based proofs and complex probabilistic arguments cannot be verified in $F^*$; on the other hand, verification in $F^*$ is fully automatic.

Moreover, EasyCrypt is not primarily designed for building, verifying and deploying large systems. Recent work [3] explores how EasyCrypt can be used to verify C implementations of well-known cryptographic constructions, and through verified compilation derive guarantees about x86 executables. However, this approach does not scale to verifying detailed protocol implementations. In contrast, $F^*$ allows programmers to combine relational and non-relational refinements freely, so that relational reasoning steps can take advantage of program invariants embedded in non-relational refinements. This distinctive ability of $F^*$ is essential to verify system implementations that rely on cryptography.

**Protocol Verification.** Blanchet’s recent account of the field of protocol verification provides a panorama of existing tools and major achievements [14]. Most of the literature focuses on verifying protocol specifications, or protocol implementations through model extractors [2]; alternatives include generating implementations from verified models [16]. Our work is most closely related to approaches that reason directly about implementations in the symbolic [12, 22] or computational models [13, 24, 31].

**Modular Type-Based Cryptographic Verification** [24]. Type systems usefully apply to many notions of security. In the context of computational cryptography, Fournet et al. rely on F7 typed interfaces to encode classic game-based security definitions, such as CPA and CCA2, using a combination of type refinements for authenticity and type abstraction for integrity and confidentiality.

In comparison, $F^*$ enables both probabilistic and relational reasoning, letting us typecheck constructions previously out of reach. In their reference implementation of TLS [13], for example, the security of several intricate cryptographic constructions is specified by typing, but justified by handwritten proofs; the corresponding code is trusted, rather than typechecked. (This is the case, e.g. for the MAC-Encode-then-Encrypt construction in the record layer, somewhat similar to our counter mode encryption example in §5.1.) We intend to carry over their 7,000 lines of code to $F^*$, reusing their detailed, classic refinements unchanged, and making use of relational typing to verify additional cryptographic libraries.

**Conclusions and Prospects.** Our work on $F^*$ represents a significant first step towards our goal of building software whose
security has been verified down to core cryptographic assumptions. On the theory side, we have shown how to generalize prior probabilistic relational logics to a higher-order language, which provides a formal basis for the use of high-level abstractions in system implementations. Practically, through careful language design, our extension of F* towards RFP* paves the way for carrying out probabilistic relational verification in a semi-automated manner using refinement types and SMT solvers. Still, much remains to be done. As immediate next steps, we anticipate extending our theory to account for dynamic allocation and local state. Toward improving our tools, on the empirical side, we plan to port an existing reference implementation of TLS [13] to RFP*. We expect that RFP*’s more flexible idioms, better support for type inference, and its self-certified kernel [43] will ease verification and allow us to push towards obtaining a high-performance implementation of the Internet standard with certified security.

References