Modular Verification of Security Protocol Code by Typing

Karthikeyan Bhargavan  Cédric Fournet  Andrew D. Gordon
Microsoft Research

Abstract
We propose a method for verifying the security of protocol implementations. Our method is based on declaring and enforcing invariants on the usage of cryptography. We develop cryptographic libraries that embed a logic model of their cryptographic structures and that specify preconditions and postconditions on their functions so as to maintain their invariants. We present a theory to justify the soundness of modular code verification via our method.

We implement the method for protocols coded in F# and verified using F7, our SMT-based typechecker for refinement types, that is, types carrying formulas to record invariants. As illustrated by a series of programming examples, our method can flexibly deal with a range of different cryptographic constructions and protocols.

We evaluate the method on a series of larger case studies of protocol code, previously checked using whole-program analyses based on ProVerif, a leading verifier for cryptographic protocols. Our results indicate that compositional verification by typechecking with refinement types is more scalable than the best domain-specific analysis currently available for cryptographic code.

Categories and Subject Descriptors F.3.1 [Specifying and Verifying and Reasoning about Programs]: Specification techniques.

General Terms Security, Design, Languages

1. Introduction

Verifying the Code of Cryptographic Protocols The problem of vulnerabilities in security protocol code is remarkably resistant to the success of formal methods. Consider, for example, the vulnerability in the public-key protocol of Needham and Schroeder (1978), first discovered by Lowe (1996) in his seminal paper on model-checking security protocols. This is the staple example of countless talks and papers on tools for analyzing security protocols. It is hence well known in the formal methods research community, and many tools can now discover it. In spite of these talks, papers, and tools, Cervesato et al. (2008) discovered that the IETF issued a public-key variant of Kerberos, shipped by multiple vendors, containing essentially the same vulnerability.

What to do? Our position is that formal tools are more likely to find such problems if they run directly on security protocol code. Most current tools require a model described in some formalism, such as a process algebra or a modal logic, but designers of new or revised protocols are resistant to writing such models. They are more concerned with functional properties like interoperability and

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright © 2010 ACM 978-1-60558-479-9/10/01... $10.00

so typically the first (and only) formal descriptions of protocol behaviour are the implementation code itself. Another reason to analyze code rather than models arises from gaps between the two: even if a model is verified, the corresponding code may deviate, and contain vulnerabilities absent from the model.

Several recent projects tackle the problem of verifying security protocol code. The pioneers are Goubault-Larrecq and Parennens (2005) who use a tool to analyze C code (written in their group) for the Needham-Schroeder public key protocol. Another early tool is FS2pv (Bhargavan et al. 2006b), which compiles implementation code in F# into the applied pi calculus, for analysis with ProVerif (Blanchet 2001), a state-of-the-art domain-specific prover. In terms of lines of code analyzed, the combination of FS2pv and ProVerif is probably now the leading tool chain for security protocol code. Several substantial case studies have yielded F# reference implementations that interoperate with existing implementations and are verified with FS2pv and ProVerif; these case studies include WS-Security (Bhargavan et al. 2006a), CardSpace (Bhargavan et al. 2008a), and TLS (Bhargavan et al. 2008b).

Towards Modular Verification It is challenging to verify security properties by compositional analysis. In particular, for systems involving cryptographic communication protocols, realistic attacker models tend to break modularity and abstraction: the attacker may interact at different layers in the protocol stack, for instance by injecting low-level network messages and controlling high-level actions at the application layer. Moreover, the attacker may compromise parts of the system, for instance gaining access to some cryptographic keys, and we are especially interested in the security properties that still hold in such situations. Accordingly, all protocol verification tools to date rely on high-complexity algorithms that operate on a complete description of the protocol.

The figure above presents the structure of our CardSpace implementation (our main case study), with one box for each F# module. Intuitively, the security properties for these modules are largely independent. Still, the earlier verification using FS2pv ignores this programming structure and passes a single, giant, untyped pi pro-
cess to ProVerif. On the one hand, ProVerif scales surprisingly well: it often succeeds on input files orders of magnitude longer than the examples in its test suite. On the other, its whole-program analysis has long run times on large case studies such as CardSpace and TLS. Analysis may take hours, or diverge, and small changes in input files have unpredictable effects on run time.

In this paper, we aim for a modular and scalable technique that avoids whole-program analysis. We develop a new methodology, based on logical invariants for the cryptographic structures arising in security protocols. We show how to implement this methodology by typechecking with refinement types, and make several improvements to the existing typechecker F7 (Bengtson et al. 2008).

By proposing a new pattern of using if F7 we intend that this paper may vindicate the promise of our initial work on refinement types for secure implementations, and establish that F7 supports scalable and flexible verification. It is flexible because we can formalize as wide a range of cryptographic operations as in F52rv, for example. It is scalable because the time consuming part of analysis, automated theorem proving, is done compositionally by repeatedly calling an external solver on relatively small logical problems.

Our Method: Invariants for Cryptographic Structures

As in the standard method originated by Dolev and Yao (1983), we model cryptographic structures as elements of a symbolic algebra. As in other logical approaches (for example, Paulson 1998, Cohen 2000, and Blanchet 2003), we rely on event predicates to record progress of a protocol run (whether or not it is public) only if the predicate $\text{Bytes}(x)$ holds. For another example, a byte array $x$ is known to the adversary only if the predicate $\text{Send}(a, b, x)$ holds. For an example of an event predicate, consider the simple protocol where $a$ and $b$ share a key $k_{ab}$, and $a$ authenticates each message sent to $b$ by sending also its hash keyed with $k_{ab}$, then the event predicate $\text{Send}(a, b, x)$ holds only if $a$ has started the protocol with the intention of sending message $x$ to $b$.

The first key idea of our approach is to rely systematically on preconditions to define invariants on cryptographic structures. For example, byte array $x$ exists in a protocol run (whether or not it is public) only if the predicate $\text{Bytes}(x)$ holds. For another example, a byte array $x$ is known to the protocol compliant principals $a$ and $b$ for the purpose of running our example protocol only if the predicate $\text{KeyAB}(k_{ab}, a, b)$ holds. Our definitions support deduction of useful properties of these invariants. For instance, in the simple case when all principals share an unsecured key and $a$ and $b$ for the purposes of running our example protocol, the predicate $\text{KeyAB}(k_{ab}, a, b)$ implies that $\text{Send}(a, b, x)$, and $\text{KeyAB}(k_{ab}, a, b)$ implies that $\text{Hash}(k_{ab}, x)$, and $\text{Hash}(k_{ab}, x)$ implies that $\text{Send}(a, b, x)$. This property captures the intuition that, if we can exhibit a byte array $x$ that has been hashed with the key $k_{ab}$, then it can only have been hashed by $a$, during a run of the protocol in which $x$ intends to send $x$ to $b$.

The second key idea is to rely on pre- and post-conditions on cryptographic algorithms to ensure that the actual code of a security protocol maintains these invariants. In our example, the precondition on applying the $\text{hash}$ function to argument $k_{ab}$ and $x$ is the formula $\text{KeyAB}(k_{ab}, a, b) \land \text{Send}(a, b, x)$, and as a postcondition, we obtain $\text{Bytes}(\text{Hash}(k_{ab}, x))$. A consequence of the implication stated above, we obtain $\text{Send}(a, b, x)$ as a postcondition of hash verification with a key satisfying $\text{KeyAB}(k_{ab}, a, b)$.

We develop our invariants as a collection of predicates defined by axioms in first-order logic. The axioms form inductive definitions of our predicates; during automated code verification we rely on the axioms as well as additional formulae proved to hold in all reachable states.

Our theory is inspired by prior work on proving secrecy and authentication by using domain-specific type systems (Abadi 1999; Gordon and Jeffrey 2003b). Intuitively, the essence of these type systems is a collection of inductive definitions that define invariants preserved by computation. Our work can be understood, in part, as an extraction of this essence as direct inductive definitions of predicates, largely independent of the host language.

Scalable Verification by Typechecking with F7

We implement and evaluate our method for F# a dialect of ML. We rely on the F7 typechecker, which verifies F# programs against types enhanced with logical specifications. A refinement type is a base type qualified with a logical formula: the formula can express invariants, preconditions, and postconditions. F7 relies on type annotations, including refinements, provided in specific interface files. While checking code, F7 generates many logical problems which it solves by submitting to Z3, an external theorem prover for first-order logic (de Moura and Björner 2008). Finally, F7 erases all refinements and yields ordinary F# modules and interfaces.

Our original paper on F7 (Bengtson et al. 2008) reported the underlying type theory, and a treatment of cryptography based on refinements types, public and tainted kinds (Gordon and Jeffrey 2003b), and seals (Morris 1973). It proposed refinement types as a means for checking security properties in general; one example showed how to enforce access control by typing, others concerned a limited repertoire of cryptographic operations. The cryptographic library described in this paper is far more expressive.

We adopt F7 as a basis for implementing our method; refinement types are an excellent way to blend typechecking with verification, still, although effective, both the theory of kinds and the use of seals necessarily depend on details of the host programming language. (Kinds are predicates on the syntax of types, and seals are $\lambda$-abstractions, only available in certain languages.) Therefore, we implement our new method, based on invariants for cryptographic structures, using F7 without seals and without the theory of kinds.

Another reason to choose F# is to enable a direct comparison with Fs2rv and ProVerif, using previously-mentioned refinement implementations for WS-Security and CardSpace. We develop our new method for cryptographic libraries that extend those already supported by Fs2rv. Thus, we illustrate the flexibility of our method, and we can experimentally measure its performance versus ProVerif. Still, our method relies on user-supplied program invariants (within refinement types), while ProVerif can infer invariants. The previous F7 theory based on kinds and seals relied on a different cryptographic library, which did not allow a comparison with Fs2rv code. To the best of our knowledge, the reference implementations checked with Fs2rv and ProVerif are currently the most sizeable body of verified code for security protocols. So implementing our method for F# and the same libraries as used with Fs2rv allows for a direct comparison against what is probably the state of the art.

Summary of Contributions

(1) A new modular method for verifying the code of security protocols, based on invariants for cryptographic structures.

(2) An implementation for the F# language by embedding invariants as refinement types, verified by the F7 typechecker.

(3) A collection of well-typed refined modules for cryptographic primitives and constructions, more expressive than in previous work with F7.

(4) Experimental evidence that typechecking is faster and succeeds on more protocol code than whole-program analysis with the leading automatic prover ProVerif.

Contents Section 2 reviews F7. Section 3 illustrates our method on an RPC protocol. Section 4 provides a theory to justify proofs of security by typechecking. Section 5 gives examples of cryptographic libraries. Section 6 outlines more substantial case studies. Section 7 evaluates the performance of our implementation. Section 8 discusses related work.
2. RCF, the Formal Foundation for F7 (Review)

We begin with a review of the syntax and semantics of RCF (Bengtson et al. 2008), our core language for F#. RCF consists of the standard Fixpoint Calculus (Gunter 1992; Plotkin 1985) augmented with local names and message-passing concURRENCY (as in the pi calculus) and with refinement types. Formally, we slightly simplify the original calculus by omitting the use of public and tainted kinds.

We state some syntactic conventions. Our phrases of syntax may contain three kinds of identifier: type variables \( \alpha \), value variables \( x \), and names \( \nu \). We identify phrases of syntax up to consistent renaming of bound identifiers. We write \( \psi \phi \) for the capture-avoiding substitution of the phrase \( \phi \) for each free occurrence of identifier \( \nu \) in the phrase \( \psi \). We say a phrase is closed to mean that it has no free type or value variables (although it may contain free names).

Expressions and types of RCF contain formulas \( C \) to specify intended properties. Specification formulas are written in first-order logic with equality, with intended properties. Specification formulas are written in first-order logic with equality, with intended properties. Specification formulas are written in first-order logic with equality, with intended properties.

Much of RCF is standard functional notation. Expressions are in the style of A-normal form; let-expressions are for sequencing and not for polymorphism. In the style of the pi calculus, RCF includes restriction (name generation), fork, and multiple transmission and reception for communication and concURRENCY. Names range over countable, pairwise-distinct constants, used to represent channels, fresh values, and keys, for instance.

An expression context \( X \) is an expression with a hole ‘ \( . \) ’. We write \( X[A] \) for the outcome of filling the hole with expression \( X \) or expression context \( A \), where variables free in \( A \) may be bound by binders in \( X \). (We use expression contexts to represent modules.)

The expressions assume and assert have no observable effect at run-time, and are used only to specify logic-based safety properties. Execution of assume \( C \) limits attention to logical interpretations in which \( C \) holds. Assumptions are used to state inductive definitions or to record events, for example. Execution of assert \( C \) indicates an error unless \( C \) holds in interpretations satisfying the previously executed assertions.

The type system of RCF is based on FPC, but with dependent function and pair types, plus refinement types \( x : T(C) \). The values of this type are the values \( M \) of type \( T \) such that \( C[M/x] \) holds.

Core Syntax of Types of RCF:

As detailed by Bengtson et al. (2008), RCF supports standard encodings of a wide range of F# programming constructs, including let-polymorphism (eliminated by code duplication), mutable references (channels), and algebraic types (recursive sums of product types); it is closely related to the internal language of the F7 typechecker. Our code examples rely on these encodings.

In addition, code written in RCF has access to a few pre-defined trusted libraries, depicted at the bottom of the figure on the first page. The library module Data defines standard datatypes such as strings, bytestrings, lists, options, and provides functions for manipulating and converting between values of these types; Crypto provides primitive cryptographic operations; Db provides functions for storing and retrieving values from a global, shared, secure database; Xml provides functions and datatypes for manipulating XML documents; Net provides functions for establishing TCP connections and exchanging messages over them. We write Lib for the composition of Data, Net, and Crypto, and LibX for the composition of Lib, Db, and Xml. These libraries are trusted in the sense that their concrete implementations are not verified. Instead, we define idealized symbolic implementations, in the style of Dolev and Yao (1983), for each of these five modules and show that they meet their typed RCF interfaces.

Each judgment of the RCF type system is given relative to an environment, \( E \), which is a sequence \( \mu_1 \ldots \mu_n \) where each \( \mu_i \) may be a subtype assumption \( \alpha \leq \alpha' \), an abstract type \( \alpha \), or an entry for a name \( x \in T \) or a variable \( x : T \). The two main judgments are subtyping, \( E \vdash T' \leq T \), and type assignment, \( E \vdash A : T \). The full rules for these judgments and the rest of RCF are in the companion technical report.

F7 relies on various type inference algorithms, and calls out to Z3 to handle the logical goals that arise when checking refinements. F7 adds the formula \( C \) to the current logical environment when processing assume \( C \), and conversely checks that formula \( C \) is provable when processing assert \( C \).
3. Invariants for Authenticated RPCs (Example)

We consider a protocol intended to authenticate remote procedure calls (RPC) over a TCP connection. We first informally discuss the security of this protocol and identify a series of underlying assumptions. We then explain how to formalize these assumptions, and how to verify an implementation of the protocol.

Informal Description

We have a population of principals, ranged over by $a$ and $b$. The security goals of our RPC protocol are that (1) whenever a principal $b$ accepts a request message $s$ from $a$, principal $a$ has indeed sent the message to $b$ and, conversely, (2) whenever $a$ accepts a response message $t$ from $b$, principal $b$ has indeed sent the message in response to a matching request from $a$.

To this end, the protocol uses message authentication codes (MACs) computed as keyed hashes, such that each symmetric MAC key $k_{ab}$ is associated with (and known to) the pair of principals $a$ and $b$. Our protocol may be informally described as follows.

An Authenticated RPC Protocol:

1. $a \rightarrow b$: utf8 $s$ | (hmacsha1 $k_{ab}$ (request $s$))
2. $b \rightarrow a$: utf8 $t$ | (hmacsha1 $k_{ab}$ (response $s$ $t$))

In this protocol narration, each line indicates the communication of data from one principal to another. This data is built using five functions: utf8 marshals the strings $s$ and $t$ into byte arrays (the message payloads); request and response build message digests (the authenticated values); hmacsha1 computes keyed hashes of these values (the MACs); and ‘’ concatenates the message parts.

We consider systems in which there are multiple concurrent RPCs between any principals $a$ and $b$ of the population. The adversary controls the network. Some keys may also become compromised, that is, fall under the control of the adversary. Intuitively, the security of the protocol depends on the following assumptions:

(1) The function hmacsha1 is cryptographically secure, so that MACs cannot be forged without knowing their key.

(2) The principals $a$ and $b$ are not compromised—otherwise the adversary may just use $k_{ab}$ to form MACs.

(3) The functions request and response are injective and their ranges are disjoint—otherwise, an adversary may for instance replace the first message payload with utf8 $s'$ for some $s' \neq s$ such that request $s' = request s$ and thus get $s'$ accepted instead of $s$, or use a request MAC to fake a response message.

(4)
Modelling the Opponent We model an opponent as an arbitrary program with access to a given public interface that reflects all its (potential) capabilities. Thus, our opponent has access to the network (modelling an active adversary), to the cryptographic library (modelling access to the MAC algorithms), and to a protocol-specific setup function that creates new instances of the protocol for a given pair of principals. This function returns four capabilities: to run the client with some payload, to run the server, to corrupt the client, and to corrupt the server (that is, here, to get their key). We detail the code for setup below: it allocates a key, specializes our client and server functions, and leaks that key upon request after assuming an event that records the compromise of either a or b.

Protocol-Specific Implementation for the Opponent Interface:

```
let setup (a:string) (b:string) =
    let k = mkKeyAB a b in
    (fun s -> client a b s),
    (fun s -> assume (Bad(a)); k),
    (fun s -> assume (Bad(b)); k)
```

Formally, the opponent ranges over arbitrary F# code well-typed against an interface that includes (at least) the declarations below. Let an opponent be an expression containing no assume or execute. Our opponent interfaces declare functions that operate on types of the form $x:T \{ Pub(x) \}$; intuitively, these types reflect the global invariant that the opponent may obtain and construct at most the cryptographic values tracked as public in our logic model. Hence, bytespub is defined as $x$: bytes $\{ Pub(x) \}$. The types strpub and keypub of public strings and public keys are defined similarly.

In our method, we explicitly give an inductive definition of Pub, and the typechecker ensures that, whenever an expression is given a public type (for instance when sending bytes on a public network), the fact that the value will indeed be public logically follows from that inductive definition.

Opponent Interface (excerpts):

```
val send: conn $\rightarrow$ bytespub $\rightarrow$ unit
val recv: conn $\rightarrow$ bytespub
val hmacsha1: keypub $\rightarrow$ bytespub $\rightarrow$ bytespub
val hmacsha1Verify: keypub $\rightarrow$ bytespub $\rightarrow$ bytespub $\rightarrow$ unit
val setup: strpub $\rightarrow$ strpub $\rightarrow$
    (strpub $\rightarrow$ unit) $\times$ (unit $\rightarrow$ unit) $\times$ (unit $\rightarrow$ keypub) $\times$ (unit $\rightarrow$ keypub)
```

As explained next, we will make more refined interfaces for typechecking our code: each value declaration will be given a refined type that is a subtype of the one listed in the opponent interface.

We are now ready to formally state our target security theorem for this protocol. We say that an expression is semantically safe when every executed assertion logically follows from previously-executed assumptions. Let $I_a$ be the opponent interface for our library. Let $I_b$ be the opponent interface for our protocol (the setup function displayed above). Let $X$ be the expression context representing the composition of the library with the protocol implementation. (We give a precise definition of $X$ in Section 4.)

**Theorem 1** For any opponent $O$, if $I_a, I_b, \vdash O : unit$, then $X(O)$ is semantically safe.

Refinement-Typed Interface for MACs Our example theorem relies on typechecking our library and protocol code against their opponent interfaces. For the library, this is done once for all, using an intermediate, more refined interface that operates on values that are not necessarily public. This interface and its logical model are explained in the companion technical report, so here we only outline their declarations and formulas as regards MACs. So the main task for verifying the RPC protocol is to typecheck it.

We first outline the refined interface for MACs, then explain how to define and enforce a logical model for the RPC protocol.

**Refinement Types for MACs (from the Crypto library):**

```
private val hmac_keygen: unit $\rightarrow$ keypub $\{ MkKey(k) \}$
val hmacsha1:
    k-key $\rightarrow$
    b-bytes $\{ MkKey(k) \wedge MACSays(k,b) \wedge (Pub(k) \wedge Pub(b)) \} $\rightarrow$
    b-bytes $\{ IsMAC(k,k,b) \wedge (Pub(k) \Rightarrow Pub(b)) \}$
val hmacsha1Verify:
    k-key $\{ MkKey(k) \wedge Pub(k) \} $\rightarrow$b-bytes $\rightarrow$b-bytes $\rightarrow$ unit $\{ IsMAC(k,h,b) \}$
(C1. By expanding the definition of IsMAC)
```

This interface defines functions for creating keys, computing MACs, and verifying them. (The private modifier indicates that a value is not included in the opponent interface.) It is designed for flexibility; simpler, more restrictive interfaces may be obtained by subtyping, for instance, when key compromise need not be considered. Its logical model is built from the following predicates:

- **MKey** $k$ records that $k$ has been produced by hmac_keygen; the adversary can produce other public keys from public values.
- **MACSays** $k,b$ is defined by the protocol that relies on $k$, as its precondition for computing a MAC and its postcondition after verifying a MAC.
- **IsMAC** $k,h,b$ holds when verification that $h$ is a MAC for $b$ under $k$ succeeds; it implies either **MACSays** $k,b$ or **Pub** $b$.

The precondition of **hmacsha1** is a disjunction that covers two cases for the key: either it is a correctly-generated key, or the key is public. The latter case is necessary to type MAC computations using a key received from the opponent, and to show that **hmacsha1** has the type declared in the opponent interface. (In type systems without formulas, such disjunctions in logical refinements could instead be expressed using union types.) The postcondition **Pub** $b$ $\Rightarrow$ **Pub** $b$ states that the MACs produced by the protocol are public (hence can be sent) provided the plaintext is public. Cryptographically, this reflects that MACs provide payload authentication but not secrecy.

The precondition of **hmacsha1Verify** similarly covers the two cases for the key. A call **hmacsha1Verify** $k,h,b$ raises an exception in case the supplied hash $h$ does not in fact match the MAC of $b$ with the key $k$. (At present, F7 does not support exception handling, and treats an exception as terminating execution.) Otherwise, its postcondition also leads to a disjunction (corollary C1), so the protocol that verifies a MAC must also know that **Pub** $b$ $\Rightarrow$ **MACSays** $k,b$, for example because $k$ is not public, to deduce that **MACSays** $k,b$.

The library also assumes definitions and theorems relating these predicates, and in particular the inductive definition of Pub. For convenience, the display above includes two properties for MACs that are corollaries of these definitions: C1 just inlineps the definition of IsMAC; C2 expresses a secrecy invariant for MAC keys: a key $k$ is public if and only if its associated logical payload holds for any value. Hence, as a prerequisite for releasing a key $k$ as a public value, a protocol must ensure that all potential consequences of MAC verification with key $k$ hold. Depending on how the protocol defines MACSays, this may be established by assuming some compromise at the protocol level (predicate **Bad** $a$) in our protocol.

**Logical Invariants for the RPC Protocol** To verify a protocol, we state some of its intended logical properties (both defining its specific usage of cryptography and stating theorems about it), we typecheck the protocol code under those assumptions, and, if need be, we prove protocol-specific theorems, as illustrated below.
We first introduce two auxiliary predicates for the payload formats: Requested and Responded are the (typechecked) postconditions of the functions request and respond; we omit their definition. Typechecking involves the automatic verification that our formatting functions are injective and have disjoint ranges, as explained in informal assumption (3). Verification is triggered by asserting the formulas below, so that Z3 proves them.

Properties of the Formatting Functions request and respond:

(request and response have disjoint ranges)
\[ \forall v', v, s', t'. \, (\text{Requested}(v) \land \text{Responded}(v', s', t')) \implies (v \neq v') \]
(request is injective)
\[ \forall v', s', t'. \, (\text{Requested}(v') \land \text{Requested}(v', s') \land v = v') \implies (s = s') \]
(response is injective)
\[ \forall v', s', t'. \, (\text{Responded}(v', s', t') \land v = v') \implies (s = s' \land t = t') \]

For typechecking the rest of the protocol, we can instead assume these formulas; this confirms that the security of our protocol depends only on these properties, rather than a specific format. In addition, typechecking involves the following three assumptions:

Formulas Assumed for Typechecking the RPC protocol:

\begin{align*}
\text{(KeyAB MACSays)} & \quad \forall a, b, k, m. \text{KeyAB}(a, b, k) \Rightarrow (\text{MACSays}(k, m) \land (a = \text{Request}(m) \lor \text{Request}(a, b, k) \lor (b = \text{Response}(a, b, k) \lor (a = \text{Responded}(a, b, k, s) \land (b = \text{Bad}(a) \lor b = \text{Bad}(b)))))) \\
\text{(KeyAB Injective)} & \quad \forall a, b, k, a', b'. \, \text{KeyAB}(a, b, k) \land \text{KeyAB}(a', b', k) \land (a = a') \land (b = b') \\
\text{(KeyAB Pub Bad)} & \quad \forall a, b, k. \text{KeyAB}(a, b, k) \land \text{Pub}(k) \Rightarrow \text{Bad}(a) \lor \text{Bad}(b)
\end{align*}

The formula (KeyAB MACSays) is a definition for the library predicate MACSays. It states the intended usage of keys in this protocol by relating MACSays to the protocol-specific predicates Request, Requested, Responded, and Bad. The definition has four cases: the MAC is for an authentic request formatted by function request, the MAC is for an authentic response to a prior request formatted by function response, or the sender is compromised, or the receiver is compromised.

The formula (KeyAB Injective) is a theorem stating that each key is used by a single pair of principals. Our informal invariant on key usage (assumption (4)) directly follows, since KeyAB(a, b, k) is a precondition of both client and server. The proof is by induction on any run of a program that assumes KeyAB only in the body of mkKeyAB. It follows from a more general property of our library: hmac_keygen returns a key built from a fresh name, hence this key is different from any value previously recorded in any event. Whenever a new event KeyAB(a, b, k) is assumed, and for any event KeyAB(a', b', k) previously assumed, we have k \neq k', so any new instance of (KeyAB Injective) holds. Conversely, we would not be able to prove the theorem if mkKeyAB also (erroneously) assumed KeyAB(a, b, k), for instance, as that might enable reflection attacks.

The formula (KeyAB Pub Bad) is a secrecy theorem for the MAC keys all located by the protocol, stating that those keys remain secret until one of the two recorded owners is compromised. This theorem validates our key-compromise model. Its proof goes as follows. Relying on the postcondition of the call to hmac_keygen within mkKeyAB, we always have \text{Key}(k) when KeyAB(a, b, k) is assumed, hence we establish the lemma \text{Key}(a, b, k, KeyAB(a, b, k) \Rightarrow \text{Key}(k)). By corollary C2, KeyAB(a, b, k) and Pub(k) thus imply that \forall m. \text{MACSays}(k, m). By inspecting (KeyAB MACSays), it suffices to show that there always exists at least one value M such that we have neither Requested(M, s) nor Responded(M, s), for any s, t. This trivially follows from the definitions of these two predicates; not every bytestring is a well-formatted request or response.

Refinement Types for the RPC Protocol Using F7, we check that our protocol code (with the Net and Crypto library interfaces, and the assumed formulas above) is a well-typed implementation of the interface below.

Typed Interface for the RPC Protocol:

<table>
<thead>
<tr>
<th>Function</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>request</td>
<td>str → payload → mbox</td>
</tr>
<tr>
<td>response</td>
<td>str → payload → mbox</td>
</tr>
<tr>
<td>service</td>
<td>payload → payload</td>
</tr>
<tr>
<td>type</td>
<td>(a : str, b : str) → keyab = k, key = (MKKey(k) \land KeyAB(a, b))</td>
</tr>
<tr>
<td>val</td>
<td>mkKeyAB : a : str → b : str → (a : str) → keyab</td>
</tr>
<tr>
<td>client</td>
<td>a : str → b : str → k : (a, b) → keyab</td>
</tr>
<tr>
<td>server</td>
<td>a : str → b : str → k : (a, b) → keyab</td>
</tr>
</tbody>
</table>

This interface is similar but more precise than the one in F#. The type payload is a refinement of string (str) that also states that the payload is a public value, so that in particular it may be sent in the clear. The value-dependent type keyab is a refinement of key that also states that the key is a MAC key for messages from a to b.

We briefly comment on the (fully automated) usage of our logical rules during typechecking.

- To type the calls to hmac_sha1, the precondition follows from the refinement in the type of k from either the first or the second disjunct of (KeyAB MACSays).
- To type the calls to send, we rely on the precondition of hmac_sha1 to show that the computed MAC is public.
- To type the leaked key k as keyab within setup, we need to show Pub(k). This follows from MKKey(k) (from the refinement in the type of k), corollary C2, and the definition of MACSays, using the just-assigned formula Bad(a) or Bad(b) to satisfy either the third or the fourth disjunct of (KeyAB MACSays).
- To type the RecvRequest protocol assertion, we must prove the formula Request(a, b, k) \lor Bad(a) \lor Bad(b) in a context where we have KeyAB(a, b, k), Requested(a, b, k), and IsMAC(k, v, s). By corollary C1, we have MACSays(k, v) \land Pub(k). By corollary C2, we have MKKey(k) \land Pub(k) \Rightarrow \forall v. MACSays(k, v), so we obtain MACSays(k, v) in both cases of the disjunction. By definition of (KeyAB MACSays), this yields

\[
\text{Requested}(v) \land \exists s. (\text{Request}(v) \land \text{Request}(a, b, s)) \lor \text{Request}(v) \land \exists s. (\text{Response}(a, b, s) \land \text{Response}(a, b, s)) \lor \text{Bad}(a) \lor \text{Bad}(b)
\]

which implies Request(a, b, k) \lor Bad(a) \lor Bad(b) by using the properties of our formatting functions.

4. Semantic Safety by Modular Typing

This section develops the theory underpinning our verification technique. First, we introduce semantic safety, which allows us to make inductive definitions of predicates in RCF. Second, we formalize F7 modules within RCF, and in particular introduce refined modules, which are modules packaged with inductive definitions of predicates and associated theorems.

Syntactic Safety by Typing (Review) We recall the operational semantics and notion of syntactic safety for RCF, together with one of the main theorems of Bengtson et al. (2008). The semantics of expressions is defined by a small-step reduction relation, written \( A \rightarrow A' \), which is defined up to structural rearrangements, written \( A \Rightarrow A' \). We represent all reachable run-time program states using expressions in special forms, named structures, ranged over by \( S \). A structure is a parallel composition of active subexpressions running in parallel, within the same scope for all restricted names. (We say a subexpression is active to mean that it occurs in evaluation context, that is, nested within restriction, fork, or let-expressions.)
In particular, from a given structure, one can extract a finite set of active assumptions and assertions. (This extraction is defined for the whole structure, up to injective renamings on the restricted names.)

- A C-structure is a structure whose active assumptions are exactly {assume $C_1, \ldots, \text{assume } C_n$} with $C = C_1 \land \cdots \land C_n$.
- A C-structure is syntactically statically safe if every RCF-interpretation to satisfy $C$ also satisfies each active assertion.
- An expression $A$ is syntactically safe if and only if, for all expressions $A'$ and structures $S$, if $A \rightarrow^* A'$ and $A' \Rightarrow S$, then $S$ is syntactically statically safe.

**Theorem 2** (Bengtson et al. 2008)

If $\emptyset \vdash A : T$, then $A$ is syntactically safe.

**Inductive Definitions and Semantic Safety by Typing** A key technique in this paper is to consider in RCF predicates given by inductive rules, such as the predicates `Byte` and `Path` mentioned in the previous section. We intend to define these predicates in RCF by assuming Horn clauses corresponding to the inductive rules. Formally, we introduce a standard notion of logic program, which is guaranteed by the Tarski-Knaster fixpoint theorem to have a least interpretation.

- A Horn clause is a closed formula $\forall x_1, \ldots, x_k (C_1 \land \cdots C_n \Rightarrow C)$ where $C_1, \ldots, C_n$ range over atomic formulas and equations and $C$ ranges over atomic formulas.
- A logic program, $P$, is a finite conjunction of Horn clauses.
- If $P$ is a logic program, let $\mathcal{F}_P$ be the least RCF-interpretation to satisfy $P$ (which exists uniquely, by Tarski-Knaster).

Syntactic safety asks assertions to hold in all interpretations that satisfy the assumptions. Instead, if we move to considering assumptions as inductive definitions, we want a weaker notion, that satisfy the assumptions. Instead, if we move to considering inductive rules, such as the predicates $\mathcal{F}_P$, we treat the concrete syntax for composing F# modules as syntactic sugar, writing $X_1 \cup X_2$ for $X_1 \cup \{X_2\}$.

An interface $I$ is a typing environment $\mu_1, \ldots, \mu_n$ where each $\mu_i$ is either an abstract type $\alpha_i$ or a variable typing $x_i : T_i$.

We lift subtyping to interfaces by the following axioms and rules, plus reflexivity and transitivity, and well-formedness conditions (so that $I \vdash I'$ always implies $I \vdash \emptyset$ and $I' \vdash \emptyset$).

- A module $X$ implements $I$ in $E$, written $E \vdash X \sim I$, when $E \vdash X.\{x_1, \ldots, x_n\} : (x_1 : T_1 \land \cdots \land x_n : T_n)$ and $(x_1 : T_1)_{\text{IF} = 1, n} = I$.

**Refined Modules** We use an expression context assumption $P \vdash Y$ to formalize the idea of a module $Y$ packaged with a (closed) logic program $P$ to make inductive definitions of predicates. We call such contexts refined modules. We want to exploit theorems following from $P$ when typechecking $Y$. To do so, we introduce the notion of a contextual theorem, a theorem that holds in any expression containing a module $P \vdash Y$ as a component.

- The support of a logic program is the set of predicate symbols occurring in the head of any clause. The support of an expression or expression context is the support of its assumptions. (Intuitively, the support is the set of predicates being defined.) Logic programs, expressions, or expression contexts are independent when their supports are disjoint.
- Let $C$ be a contextual theorem of expression context assumption $P \vdash Y$ if and only if $C$ is a theorem of assumption $P \vdash Z[Y][A]$ whenever $Z$ and $A$ are factual and independent of assumption $P \vdash Y$.

When the following lemma applies, we can prove contextual theorems from the inductive definitions of $P$'s assumption $P \vdash Y$, without explicit consideration of the operational semantics.

**Lemma 1** (Contextual). Let $C$ be a formula and $P$ a logic program such that, for all $Q$ independent from $P$, the least RCF-interpretation to satisfy $P \land Q$ also satisfies $C$. If $Y$ is an expression context independent from $P$, then $C$ is a contextual theorem of assumption $P \vdash Y$.

- Let a refined module be a triple $M = (E, X, S)$ such that there are closed formulas $M^{\text{def}}$ and $M^{\text{thm}}$, and a module $Y$ where:
  1. $X$ is factual and $X \vdash M^{\text{def}} \vdash Y$;
  2. $E, M^{\text{def}}, M^{\text{thm}} \vdash Y \sim I$;
  3. $M^{\text{thm}}$ is a contextual theorem of $X$.

(When we write a formula such as $M^{\text{def}}$ as an environment entry, we mean it as shorthand for: $\{M^{\text{def}}\}$ where the type $(M^{\text{def}}) = X := \text{unit}(M^{\text{def}})$, where each occurrence of $X$ stands for a fresh variable. This type is only populated when $M^{\text{def}}$ holds, so the effect of the entry is simply to add $M^{\text{def}}$ as a logical assumption.)

Our example relies on Lib, the composition of the library modules Data, Net, and Crypto, which together form a refined module. Let $Lib$ be the F# code of the library, that is, the composition $\text{Data Net Crypto}$ of the code of the libraries. Let $\Lambda$ be the F7 interface, which includes, for example, the functions labelled...

**Theorem 3** Consider closed expression $A$ and formula $C$ where:

1. the expression $\text{assume } C \vdash A$ is syntactically safe; and (2) $C$ is a theorem of $A$. Then $A$ is syntactically safe.
"Refinement Types for MACs" in Section 3. The inductive definitions \( \text{Lib}^{\text{def}} \) include formulas defining the \( \text{Pub} \) and \( \text{Bytes} \) predicates, while \( \text{Lib}^{\text{com}} \) includes the corollaries C1 and C2 in Section 3.

**Lemma 2** \( \text{Lib} = (\varnothing, \text{assume} \text{Lib}^{\text{def}} \cap \text{Lib}, I_1^L) \) is a refined module.

As another example, our RPC protocol consists of a refined module of the form \( \text{RPC} = (I_7^R, \text{assume} \text{RPC}^{\text{def}} \cap \text{RPC}, (I_8, I_9)) \).

Let \( \text{RPC} \) be the F# code for the protocol. The inductive definitions \( \text{RPC}^{\text{def}} \) include the right to left form of \( \text{KeyAB MACSays} \) from Section 3. The theorems \( \text{RPC}^{\text{com}} \) include \( \text{KeyAB Injective} \), \( \text{KeyAB Pub Bad} \), and the left to right form of \( \text{KeyAB MACSays} \) from Section 3. The \( \text{RPC} \) interface \((I_8, I_9)\) includes a module available to the opponent. Let \( I_9 \) be the library's opponent interface, which is not detailed in Section 3. Let \( I_9 \) be the protocol-specific opponent interface from Section 3. As mentioned in that section, the module below imports \( I_9^L \) and exports its members at the more abstract interface \( I_9 \), by introducing abstract types such as bytespub with representation type \( \text{x bytes} \{ \text{Pub}(x) \} \).

**Lemma 3** \( \text{RPC} \) is a refined module.

**Composition of Refined Modules**

- We say \( M_1 = (E_1, X_1, I_1) \) composes with \( M_2 = (E_2, X_2, I_2) \) iff \( I_1 \preceq E_2 \) and \( X_2 \) are independent.

- For any triples \( M_1 = (E_1, \text{assume} \text{MK}^{\text{def}} \cap \text{MK}, (I_1, I_9)) \) and \( M_2 = (E_2, \text{assume} \text{MK}^{\text{def}} \cap Y_1, I_2) \) their composition \( M_1; M_2 \) is the triple \( (E_1, \text{assume} \text{MK}^{\text{def}} \cap \text{MK}^{\text{def}} \cap Y_2, I_2) \).

**Lemma 4** (Composition). If refined module \( M_1 \) composes with refined module \( M_2 \) then \( M_1; M_2 \) is a refined module.

For example, the triple \( \text{Lib}; \text{RPC} \) is \( \text{Lib} \text{assume} \text{Lib}^{\text{def}} \cap \text{RPC}^{\text{def}} \cap \text{RPC}, (I_7^R, I_8) \).

**Safety and Robust Safety by Typing for Modules**

- A refined module \( (\varnothing, X, \varnothing) \) is semantically safe if and only if, the expression \( X([], 1) \) is semantically safe.

- An \( I \)-opponent is an opponent \( O \) such that \( I \vdash O : \text{unit} \).

- A refined module \( (\varnothing, X, I) \) is robustly safe if and only if, the expression \( X([O]) \) is semantically safe for every \( I \)-opponent \( O \).

**Theorem 4** (Safety). Every refined module \( (\varnothing, X, \varnothing) \) is semantically safe.

**Theorem 5** (Robust Safety). Every refined module \((\varnothing, X, I)\) is robustly safe.

We can now prove Theorem 1. We have that \( \text{Lib}; \text{RPC} = (\varnothing, X, (I_1, I_9)) \) where \( X = \text{assume} \text{Lib}^{\text{def}} \cap \text{RPC}^{\text{def}} \cap \text{RPC} \) is a refined module. By Theorem 5 (Robust Safety), \((\varnothing, X, (I_1, I_9))\) is robustly safe, which is to say that \( X([O]) \) is semantically safe for every opponent \( O \) with \( I \preceq I_9 \) and \( O : \text{unit} \).

5. **Library Modules for Cryptographic Protocols**

In this section, we describe intermediate refined modules, built on top of the Crypt module, that implement derived mechanisms and composite patterns commonly used in cryptographic protocol implementations. We refer to the companion paper for a complete description, and for a detailed presentation of the Crypt module. (Section 3 also presents its interface for MACs.) Both modules are fully verified, and demonstrate the flexibility of our approach. Relying on these libraries, their logical definitions, and their theorems, we build (and verify) a series of modular protocols, leading to Windows CardSpace.

**Key Management**

The Principals library generalizes the treatment of keys and principals illustrated in the example protocol of Section 3. (To facilitate the comparison, we illustrate mostly the treatment of MAC keys.) Instead of a fixed population of principals and keys, the library maintains a database of keys shared between an extensible set of principals. Pragmatically, this functionality may be implemented using some existing public-key infrastructure, or an in-memory database recording the outcome of prior key-exchange protocols. Formally, our implementation of Principals relies on Db, a channel-based abstraction for databases. The main purpose of the library is to systematically link cryptographic keys to application-level principals, while keeping track of their potential compromise.

Principal identifiers are represented by a type \( \text{prin} \) defined as a public string. Each principal may have a number of MAC keys, encryption keys, and public/private key pairs. The library maintains a database that may be used by multiple protocols to store and retrieve keys. Keys are grouped by usage (set by the protocol that generates the key) to distinguish between the intended usage of each key, and associated with one (for public/private keypairs) or two principals. For instance, a MAC key \( mk \) managed by the library for some usage \( \text{RPc} \) shared between principals \( a \) and \( b \) is given the type \( (\text{mk} : \text{key}) \{ \text{MACKey}(\text{RPc}, a, b, mk) \} \) (where \( \text{key} \) is the type of keys in Crypto). For managed MAC keys, Principals provides functions:

- \( \text{mkMACKey} : \text{usage} \rightarrow a : \text{prin} \rightarrow b : \text{prin} \rightarrow \text{mk} : \text{key} \{ \text{MACKey}(\text{RPc}, a, b, \text{mk}) \} \)
- \( \text{genMACKey} : \text{usage} \rightarrow a : \text{prin} \rightarrow b : \text{prin} \rightarrow \text{mk} : \text{key} \{ \text{MACKey}(\text{RPc}, a, b, \text{mk}) \} \)

The function \( \text{mkMACKey} \) generates and returns a fresh MAC; \( \text{genMACKey} \) can be used to store the key in the database; \( \text{getMACKey} \) retrieves a key from the database. From these three functions, only \( \text{genMACKey} \) is available in the opponent interface.

Managed keys can be used for standard cryptographic operations. To this end, Principals links key-level predicates used in Crypto (defined by Principals) to principal-level predicates (to be defined by the protocol): \( \text{Send}(u, a, b, s) \) means that the principal \( a \) intends to MAC \( s \) before sending it to \( b \); \( \text{Encrypt}(u, a, b, s) \) records that \( s \) may be encrypted towards \( b \) using symmetric encryption; \( \text{SendFrom} \) and \( \text{EncryptTo} \) similarly record intended asymmetric signatures and asymmetric encryption with a managed key. The Principals library also provides functions for compromising keys. Compromise is dealt with at the level of principals \( \text{Bad}(a) \) indicates that principal \( a \) has been compromised, and thus that all the keys it could access may have been leaked. For MACs, for instance, the library interface assumes the formulas below:

**MAC Key Usage**

\[
\begin{align*}
\text{MACKeyMACSays Send} \\
\forall a, b, m, s. \text{MACKey}(a, b, m) \wedge \text{Send}(a, b, m) \Rightarrow \text{MACSays}(m, s) \\
\text{MACKeyMACSays Bad} \\
\forall a, b, m, s. \text{MACKey}(a, b, m) \wedge \text{Bad}(a) \Rightarrow \text{MACSays}(m, s) \\
\text{InvMACKeyMACSays} \\
\forall a, b, m, s. \text{MACKey}(a, b, m) \Rightarrow \text{MACSays}(m, s) \\
\text{MACKeySecrecy} \\
\forall a, b, m, s. \text{MACKey}(a, b, m) \Rightarrow \text{MACSays}(m, s) \\
\end{align*}
\]

The two first clauses are definitions, enabling hmacsha1 to be called with a managed MAC key once the protocol has assumed an adequate definition of Send, with a more liberal precondition in case of compromise. The third and fourth clauses are theorems: MAC verification with a managed key yields a principal-level guar-
antee; and a MAC key shared between two principals remains secret until one of them gets compromised.

Our model of key compromise is among the most general models for protocol verification. It supports three kinds of keys: those generated by the attacker, those generated by the principals’ library and kept secret, and those generated by the principals’ library and leaked to the attacker. It allows cryptographic operations to be performed with all three categories of keys. Moreover, all keys may be encrypted, MACed, or signed under other keys. For instance, if a key is used to encrypt some collection of other keys (as tracked by Send), our logical model rightfully demands, as a precondition for compromising any principal with access to that key, that the conditions for leaking each of these encrypted keys be also recursively satisfied. Although this leads to complex refinement types and assumptions, most of this complexity is factored out in the library and can be used with a low overhead.

Recall that LibX is the composition of Lib, Db, and XmL.

**Lemma 5** LibX: Principles is a refined module.

**Authenticated Encryption** The Crypto module provides plain (unauthenticated) symmetric encryption:

Refinement Types for Encryption (from the Crypto library):

```plaintext
private val aes_keygen: unit → k: key(SKey(k))
val aes_encrypt: (aes CBC →) k: key → b: bytes (SKey(k) ∧ CanSymEncrypt(k,b)) → (Pub(k) ∧ Pub(b)) → e: bytes (IsEncryption(e,k,b))
val aes_decrypt: (aes CBC →) k: key, (SKey(k) ∨ Pub(k)) → e: bytes → b: bytes (IsSymEncrypt(e,k,b) → b = mp) ∧ (Pub(k) ⇒ Pub(b))
```

The function aes_keygen generates symmetric keys, logically tracked by SKey; aes_encrypt can be called in two ways: either with a “good” key generated by aes_keygen and a plaintext b such that CanSymEncrypt(k,b) holds, or with any public and a known to or provided by the attacker); it returns encrypted bytes e, tracked by IsEncryption; aes_decrypt takes a key k and bytes e and extracts a plaintext b. Since encryption is unauthenticated, decryption may succeed even if e is not a valid encryption, returning some unspecified garbage bytes, so the first postcondition of aes_decrypt just says that, if the caller knows that e is an encryption of some (possibly unknown) plaintext p under e, then decryption does returns p. (The second postcondition enables re-encodings.)

The Patterns module shows how to derive authenticated encryption, for each of the three standard composition methods for encryption and MACs (see, e.g., Bellare and Namprempre 2008).

**Encrypt-then-MAC (as in IPSEC in tunnel mode):**

```plaintext
a → b: e | hmacsha_k1 m_a e where e = aes k_0 t
```

**MAC-then-Encrypt (as in SSL/TLS):**

```plaintext
a → b: aes k_0 (b | hmacsha_k1 m_a)
```

**MAC-and-Encrypt (as in SSH):**

```plaintext
a → b: aes k_0 t | hmacsha_k1 m_a t
```

Depending on the method, the message is first encrypted, then the encryption is MACed, or the message is first MACed and then both the message and the MAC are encrypted, or the message is first MACed but the MAC is left unencrypted. For each method, the goal is to securely communicate plaintexts; from a to b relying on pre-established shared keys, but the underlying cryptographic assumptions slightly differ. Cryptographers prefer the first method, as it prevents chosen-ciphertext attacks and does not require secrecy assumptions on the MAC function. We implemented and verified all three (using a secrecy-preserving MAC in the third case, as expected). We focus on encrypt-then-MAC, since this was not implementable in our previous work with F7.

**Authenticated Encryption API:**

```plaintext
val authenc_keygen: unit → (ek: key; mk: key) (AuthEncKeyPair(ek,mk))
val authenc_decrypt: (ek: key; mk: key) → b: bytes (AuthEncKeyPair(ek,mk) ∧ CanSymEncrypt(ek,b)) → (Pub(ek) ∧ Pub(mk) ∧ Pub(b)) → e: bytes (IsAuthEncryption(e,ek,mk,b))
val verify_auth_decrypt: (ek: key; mk: key; (AuthEncKeyPair(ek,mk) ∧ CanSymEncrypt(ek,b))) → e: bytes → b: bytes (IsAuthEncryption(e,ek,mk,b) ∧ (Pub(ek) ⇒ Pub(b)))
```

The function AuthEncKeyPair links pairs of keys for the method; encryption returns a concatenation of an encryption and a MAC, tracked by IsAuthEncryption. verify_auth_decrypt has a stronger postcondition than aes_decrypt; its result must have been encrypted using encrypt-then-mac, thereby excluding garbage. To verify these functions and obtain both integrity and confidentiality for b, for each key pair, we link MACSays(mk,b) and CanSymEncrypt(ek,b) to get both integrity and confidentiality for b:

**Authenticated Encryption Key Usage:**

```plaintext
(AuthEncKeyPair MacSays)
∀mk,ek,b.p, AuthEncKeyPair(ek,mk) ∧ IsEncryption(e,ek,p) ∧ CanSymEncrypt(ek,b) ⇒ MACSays(mk,b)
```

The correctness of verify_auth_decrypt relies on theorems stating that this is the only use of these keys, and linking their potential compromise.

**Hybrid encryption** Hybrid encryption is the standard method of implementing public-key encryption for large plaintexts: generate a fresh symmetric key; use it to encrypt the plaintext; then encrypt the key using the public key of the intended receiver.

**Hybrid Encryption:**

```plaintext
a → b: rsa_rsaep pk_b, k_a | aes k_0 t
```

This hybrid encryption combines authenticated asymmetric encryption (RSA-OAEP) with unauthenticated symmetric encryption, and provides authenticated asymmetric encryption (analogous to RSA without OAEP). The library has three functions for it:

**Hybrid Encryption API:**

```plaintext
val hybrid_keygen: unit → (pk: key; sk: key) {HyPubKey(pk) ∧ HyPrivKey(sk) ∧ PubPrivKeyPair(pk,sk)}
val hybrid_encrypt: k: key → b: bytes {HyPubKey(k) ∧ CanHyEncrypt(k,b)} → (Pub(k) ∧ Pub(b)) → e: bytes (IsHyEncryption(e,k,b))
val hybrid_decrypt: sk: key → b: bytes (HyPubKey(k) ∧ CanHyEncrypt(k,b) ∧ Pub(k) ∧ Pub(b)) → e: bytes (IsSymEncrypt(e,sk) → b = mp) ∧ (Pub(sk) ⇒ Pub(b))
```

Their code is straightforward, but their verification is challenging (since it must rely on the assumption that the symmetric key is used for a single hybrid encryption). Predicates HyPubKey, HyPrivKey, and HySymKey track the three kinds of keys used in the code. The protocol-defined predefinition of hybridEncrypt is linked to the underlying CanSymEncrypt and CanAsymEncrypt cryptographic predicates as follows:

**Hybrid Encryption Key Usage:**

```plaintext
(HyPubKey CanAsymEncrypt)
typically (pk,bk, HyPubKey(pk) ∧ HySymKey(SymKey(bk),pk) ⇒ CanAsymEncrypt(pk,bk))
```

```plaintext
(HySymKey CanSymEncrypt)
typically (pk,bk, HySymKey(pk,bk) ∧ CanHyEncrypt(pk,bk) ⇒ CanSymEncrypt(pk,bk))
```
To typecheck hybridDecrypt, we establish theorems stating that hybrid encryption keys are used only as above, and linking the compromise of the inner symmetric encryption key to that of the outer private key. After hiding auxiliary predicates, hybrid encryption has exactly the same interface as plain RSA in Cryptol, showing that the derivation does not entail any loss of flexibility.

**Derived Keys and Endorsing Signatures** The library also provides support for deriving separate keys from a secret seed, and for endorsing signatures (that is, composing MACs and asymmetric signatures).

**LEMMA 6 LibX; Patterns is a refined module.**

**Example: The Otway-Rees Protocol** Using the Principals and Patterns libraries, we can build up several protocol implementations and establish their security with minimal effort. We outline our implementation of the Otway-Rees protocol, a well-known academic protocol for establishing a fresh short-term key between two principals a and b.

**Otway-Rees Protocol:**

1. \( a \rightarrow b \): `id | a | b | aenc ka (na | id | a | b)`
2. \( b \rightarrow s \): `id | a | b | aenc ka (na | i+1 | id | a | b)`
3. \( s \rightarrow b \): `aenc kb (nb | id | a | b)`
4. \( b \rightarrow a \): `id | aenc ka (na | kab)`

Here, `aenc k x stands for the authenticated encryption of x under the key pair k, implemented using the Encrypt-Then-MAC mechanism. Using Principals we create a population of principals, ranging over by \( p \) together with a server \( s \). The server shares a set of long-term key pairs with principals. Each long-term key pair \( k_p \) is associated with and known to principal \( p \) and to \( s \).

The main authentication goal is that \( a, b, s \) agree on all the main parameters of the protocol: the principals involved, \( a, b, s \), the session identifier \( i \), and the established key \( kab \). The main secrecy goal is that \( kab \) must be known only to \( a, b, s \). These goals are established mainly by typing the code against the Principals and Patterns interfaces. The only theorems proved by hand state the freshness of nonces and keys generated in the protocol.

**LEMMA 7 LibX; Patterns; Principals; OtwayRees is a refined module.**

**Example: Secure Conversations** Next, we build a protocol for authenticated conversations between two principals. To illustrate compositionality, the key k is established by the Otway-Rees protocol, then used for authenticated encryption, as described above.

**Session Sequence Integrity (initially \( i = 1 \)):**

\[
i . a \rightarrow b : id | aenc k (i | m_i) \\
i + 1 . b \rightarrow a : id | aenc k (i + 1 | m_{i+1})
\]

After key establishment, the conversation protocol loops between request and response messages, incrementing a sequence number at each step. The authentication goal is that \( a \) and \( b \) must agree on the full sequence of messages \( (m_i)_{i \geq 1} \) sent and received (possibly excluding the last message in transit). Verification of such unbounded protocols is typically beyond the reach of automated verification tools, since it requires a form of induction. Nonetheless, we are able to implement and verify this protocol by typing, relying on recursive predicates that record the entire history of the session, and show that the local histories at both \( a \) and \( b \) are consistent.

**LEMMA 8 LibX; Patterns; Principals; OtwayRees; Sessions is a refined module.**

6. **Case Study: Windows CardSpace**

We describe our main case study, verifying an implementation of the federated identity-management protocol Windows CardSpace. The protocol consists of three roles, a client \( C \), a web server (named relying party \( RP \)), and an identity provider \( IP \). To access \( RP \), \( C \) first obtains an identity token from \( IP \), and then uses this token to authenticate its messages to \( RP \). Hence, the protocol uses two message exchanges, between \( C \) and \( IP \) then between \( C \) and \( RP \). Structurally, CardSpace is similar to many other server-based identification protocols, such as Kerberos, Passport, and SAML. A distinguishing feature is that it is built using the standard mechanisms of web services security.

Our code is written in F# and was developed for an earlier verification case study (Bhargavan et al. 2008b) using ProVerif. Its modular structure is shown in the figure on the first page. In addition to the trusted libraries LibX and the protocol libraries Principals and Patterns, the implementation consists of library modules implementing various web services security specifications and modules implementing the CardSpace protocol. (We added type annotations, but did not need to change any code for the XML protocol stack.)

**Flexible Message Formats: XML Digital Signatures** In standardized protocols such as CardSpace, most of the programming effort is in correctly implementing the message formats for interoperability. Protocols built on web service security must also deal with the inherently flexible nature of the XML message format.

An XML signature is far more than a few bytes containing a MAC or signature value: it carries XML metadata indicating how those bytes were computed (in two stages) and how to use the signature. For the first stage, it embeds a list of references to the XML elements it is authenticating, a cryptographic hash of each of these elements, and the names of algorithms used to canonicalize and hash those elements; for the second stage, it embeds a signature computed on those hashes, its algorithm, and a reference to its signing key. For example, a typical signature of n elements \( i, \ldots, i_n \) in an RSA signing key ska takes the form:

```xml
<Signature>
  <SignedInfo>
    ...<SignedInfo>
</Signature>
```

```xml
<Reference uri="#1"/>
  <Transforms>
    <Transform Algorithm="C14n"/>
  </Transforms>
  <DigestMethod Algorithm="SHA1"/>
  <DigestValue>
    base64 (sha1 (utf8 (c14n si1)))
  </DigestValue>
</Reference>
```

```xml
<Reference uri="#n"/>
</Reference>
```

```xml
<SignedInfo>
  <SignatureValue>
    base64 (rsa_sign ska (utf8 (c14n si1)))
  </SignatureValue>
  <KeyInfo>
    a's X.509 Certificate ...
  </KeyInfo>
</SignedInfo>
```

To process such a signature, the verifier retrieves the elements, verification key, and the algorithms, and reconstructs the signature value. The signature may include any number of target elements, so the verifier may have to check a signature of unbounded length. This is beyond most cryptographic verification techniques: earlier analyses of XML signature protocols limit the maximum number of signed elements, essentially treating lists as tuples (Bhargavan et al. 2006a; Kleiner and Roscoe 2005). With explicit type annotations, however, we capture the full flexibility of XML signatures. We use a recursive predicate `isReferenceList` to represent the list of `<Reference>` elements, and use it to define a predicate.


**Protoocols and Libraries**

<table>
<thead>
<tr>
<th>F# Program</th>
<th>F7 Typingchecked</th>
<th>F7# Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modules</td>
<td>Interface</td>
<td>Checking Time</td>
</tr>
<tr>
<td>Trusted Libraries (Symbolic)</td>
<td>5</td>
<td>+96 lines</td>
</tr>
<tr>
<td>Princials (Section 5)</td>
<td>1</td>
<td>207 lines</td>
</tr>
<tr>
<td>Cryptographic Patterns (Section 5)</td>
<td>1</td>
<td>250 lines</td>
</tr>
<tr>
<td>Otway-Rees (Section 5)</td>
<td>2+1</td>
<td>+234 lines</td>
</tr>
<tr>
<td>Otway-Rees (No MACs)</td>
<td>2+1</td>
<td>+265 lines</td>
</tr>
<tr>
<td>Secure Conversations</td>
<td>2+1+1</td>
<td>+123 lines</td>
</tr>
<tr>
<td>Web Services Security Library</td>
<td>7</td>
<td>1702 lines</td>
</tr>
<tr>
<td>X.509-based Client Auth (Section 6)</td>
<td>7+1</td>
<td>+88 lines</td>
</tr>
<tr>
<td>Password-X.509 Mutual Auth</td>
<td>7+1</td>
<td>+129 lines</td>
</tr>
<tr>
<td>X.509-based Mutual Auth (Section 6)</td>
<td>7+1</td>
<td>+111 lines</td>
</tr>
<tr>
<td>Windows CardSpace (Section 6)</td>
<td>7+1+1</td>
<td>+1429 lines</td>
</tr>
</tbody>
</table>

---

**IsSignedInfo** that reflects the schema of the `<SignedInfo>` element. We enforce the invariant that all messages signed with XML signature keys have the structure defined in `IsSignedInfo`. Using similar predicates, we verify modules implementing each of the needed web services security specifications. We write LibWS for our web services security library composed of LibX, Principals, Patterns, SOAP, WS-Addressing, XML-Signature, XML-Encryption, WS-Security, and WS-Trust.

**Lemma 9** LibWS is a refined module.

**Composing Cryptographic Patterns:** Secure XML Request/Response Each message exchange in CardSpace implements a secure request/response protocol built on top of the web services security library. Unlike the RPC protocol of Section 3, this protocol guarantees both authentication and confidentiality, and uses many of the composite cryptographic patterns introduced in Section 5. XML flexibility also has a cost: the message we verify are large (up to 15k) and complex (up to 17 cryptographic operations).

We describe an instance of the protocol using asymmetric keys. Assume principal $a$ has a private key $sk_a$, $b$ has a public key $pk_b$, and both $a$ and $b$ have exchanged their public keys using X.509 certificates. The protocol below uses four cryptographic patterns implemented for XML: derived keys, hybrid encryption, signature, and endorsing signatures.

**Secure XML Request/Response (X.509 Mutual Authentication):**

\[
\text{a: Generate } k_{ab}, n_1, n_2 \\
\text{1. } a \rightarrow b: r_{skk}{kab} {n_1}{n_2} \\
\text{XML-Encrypt } k_{2b} {sk_1} \text{ where } sk_1 = \text{XML-Sign } k_1 [m] \\
\text{XML-Encrypt } k_{2b} {sk_2} \text{ where } sk_2 = \text{XML-Sign } sk_1 [s] \\
\text{XML-Encrypt } k_{2b} {m_1} \\
\text{b: Generate } n_3, n_4 \\
\text{2. } b \rightarrow a: n_3 {n_4} \\
\text{XML-Encrypt } k_{4a} {s_3} \text{ where } s_3 = \text{XML-Sign } k_3 {m_2} \\
\text{XML-Encrypt } k_{4a} {m_2}
\]

Before sending the request (message 1), $a$ generates a fresh keyseed $k_{ab}$ and two nonces $n_1$ and $n_2$. It uses $k_{ab}$ and the nonces to derive a MAC key $k_1$ and an encryption key $k_2$. It signs the message $m_1$ with $k_1$ to obtain the XML signature $s_1$, and then signs $s_1$ with $sk_a$ to obtain the encoding XML signature $sk_1$. Finally, it secretly encrypts $sk_1$, $s_2$, and $m_1$ with the encryption key $k_2$. The response (message 2) is simpler: $b$ derives two keys $k_3$ and $k_4$ and uses them to sign and then encrypt the response message $m_2$.

The security goals are mutual authentication of $a$ and $b$, plus authentication and secrecy of $m_1$ and $m_2$. These goals are verified by typechecking the protocol code against the web services security library LibWS (including Patterns).

**Lemma 10** LibWS;SecureRPC is a refined module.

---

**Composing Protocols:** CardSpace We assemble CardSpace by composing two XML request/response exchanges. To avoid repeating the message formats, we abstractly represent each request message by `Request, k1 k2 [m1; . . .; mn]`, where $k_1$ and $k_2$ are the keys of the sender and recipient ($sk_a$ and $pk_b$ in the XML request/response protocol above), and $[m1; . . .; mn]$ is the list of message elements protected by the protocol ($m_1$ above). The corresponding responses are represented by `Response, [m1; . . .; mn]`.

**CardSpace Protocol (using X.509 Mutual Authentication):**

\[
1. \ C \rightarrow \ IP: \ Request, skC pkIP [TokenRequestRP, pkRP] \\
2. \ IP \rightarrow C: \ ResponseC [XML-Encrypt pkRP t] \\
3. \ C \rightarrow \ RP: \ ResponseRP [pkRP, m] \\
4. \ RP \rightarrow C: \ ResponseRP [m]
\]

In the first exchange, the client $C$ requests a token from identity provider $IP$ for use at $RP$. The $IP$ responds with a signed token $t$ (in the syntax of SAML), containing $C$’s identity information $id$, and a key $kt$ that $C$ may use at $RP$ to prove its possession of $t$. The $IP$ also encrypts $t$ for $RP$ and sends it to $C$; $C$ forwards this token in its subsequent request to $RP$, and uses the key $kt$ to authenticate the request ($m$). The $RP$ decrypts the token $t$ and checks $IP$’s signature on it to convince itself of $C$’s identity, before responding with $m_2$.

The security goal of the protocol is the authentication of $C$’s identity $id$ at $RP$, and the secrecy and authentication of $m_1$ and $m_2$.

**Lemma 11** LibWS;SecureRPC is a refined module.

---

**7. Performance Evaluation**

The table above summarizes our verification results for the protocols and libraries described in this paper. Each row lists the number of modules and lines of code in the F# protocol implementation, the number of lines in the F7 typed interface, and the time for verification by typechecking. The F7 interface extends the F# module interface with security assumptions, theorems, and goals, as well as type annotations needed for verification. For comparison, the table also lists, where applicable, the results of verifying the protocol implementation through the F5²Pv-ProVerif tool chain: it lists the number of queries (security goals) proved and their verification time. All experiments were performed on an Intel Xeon workstation with two processors at 2.83 GHz, with 32GB memory, and running Windows Server 2008. (Most of these ProVerif results have been published in earlier work.)

The first part of the table corresponds to the RPC protocol of Section 3. The first row is for the trusted libraries Lib; the * indicates that we verify their idealized symbolic implementation, not their concrete code. The second row is for the RPC protocol; since the libraries are verified once and for all, this row shows only the incremental lines of code and type checking for verifying RPC. In contrast, ProVerif verifies both Lib and RPC together. For small
examples as such, we find that the domain-specific analysis of ProVerif is faster than F7.

The second part corresponds to the libraries and protocols of Section 5. The first and second rows are for Principals and Patterns. The third row corresponds to the Otway-Rees protocol. We find that the incremental typechecking time of Otway-Rees is only 1m 29.9s, whereas ProVerif takes 8m 2.2s to verify the protocol. Even adding verification times for the libraries, we find that typechecking with F7 is much faster than ProVerif. Our typed cryptography is more realistic than typical ProVerif models; for instance it tells the difference between authenticated and unauthenticated encryption; with unauthenticated encryption, typechecking fails to verify Otway-Rees (fourth row) but ProVerif still succeeds. (Weaker assumptions can sometimes be coded in ProVerif but are not provided by default.) The protocol in the fifth row implements the unbounded secure conversations protocol. The typechecker easily verifies this recursive code, but ProVerif cannot, and fails to terminate. For recursive code, typechecking lets the programmer provide hand-written (recursive) invariants; fully automated model checkers and theorem provers (like ProVerif!) lack this facility.

The third part corresponds to protocols of Section 6, arranged in increasing complexity leading up to the CardSpace protocol. The first row presents verification results for the web services security libraries LibWSS. We then present verification results for a single-message client authentication protocol, two secure request/response protocols, and the CardSpace protocol. We find that the incremental typechecking times scales almost linearly with the size of the protocol code. In contrast, the ProVerif verification time increases exponentially with the protocol complexity (for each extra layer of encryption or signature, or each extra message). For instance, ProVerif takes less than a minute to analyze the client authentication protocol but up to an hour to verify mutual authentication protocols. The jump in analysis time is primarily because ProVerif has to account for all possible dependencies between the two messages, such as whether the adversary may use the second message of a session to compromise the first message of another session. The increase in verification complexity makes it infeasible to verify the whole CardSpace protocol using ProVerif. Indeed, in the last row of the table, the + indicates that the ProVerif verification only applies when the number of clients and servers are limited to at most two each (one honest and one compromised principal for each role) and when the full XML message formats in the web services security libraries are abstractly represented as tuples. Even with these restrictions, ProVerif takes 66m 21s to verify the protocol implementation. In contrast, typechecking incrementally verifies CardSpace in a few minutes.

We conclude that typechecking scales far better than whole-program analyses for security protocols. As a trade-off, the programmer must declare their usage of cryptography by providing annotations in the typed interface of each protocol.

8. Related Work

Fs2cv (Bhargavan et al. 2008a) is the first tool to verify properties in the computational model of implementation code of security protocols. Fs2cv generates inputs to CryptoVerif (Blanchet 2006) from the implementation code in F#. It has been applied to an F# implementation of TLS.

ASPIER (Chaki and Datta 2009) has been applied to verify properties of the code of the central loop of OpenSSL. It performs no interprocedural analysis and relies on unverified user-supplied abstractions of all functions called from the central loop. ASPIER is based on software model-checking techniques, and proves properties of OpenSSL assuming bounded numbers of active sessions.

The RCF system of refinement types is similar to that of recent systems such as SAGE (Flanagan 2006) and Dsolve (Rondón et al. 2008), although neither of these systems allows full first-order formulas as refinements. Still, we expect with a little adaptation tools such as these could support our method.

Acknowledgements François Dupressoir, Nataliya Guts, and Cătălin Hritcu suggested improvements to the paper.

References


