Abstraction and Refinement in Protocol Derivation

Anupam Datta Ante Derek John C. Mitchell Dusko Pavlovic

Computer Science Department
Stanford University
Stanford, CA 94305-9045
{*danupam,aderek,jcm*}*@cs.stanford.edu*

Kestrel Institute
Palo Alto, CA 94304

dusko@kestrel.edu

March 15, 2004

Abstract

Protocols may be derived from initial components by composition, refinement, and transformation. Using a higher-order extension of a previous protocol logic, we present an abstraction-instantiation method for reasoning about a class of protocol refinements. The main idea is to view changes in a protocol as a combination of finding a meaningful "protocol template" that contains function variables in messages, and producing the refined protocol as an instance of the template. Using higher-order protocol logic, we can develop a single proof for all instances of a template. A template can also be instantiated to another templates, or a single protocol may be an instance of more than one template, allowing separate protocol properties to be proved modularly. These methods are illustrated using some challenge-response and key generation protocol templates that also require adding symmetric encryption and cryptographic hash to the protocol logic. We show additional uses of the methodology and suggest future directions by exploring a design space surrounding JFK (Just Fast Keying) and related protocols from the IKE (Internet Key Exchange) family. This exploration reveals some trade-offs between authentication, identity protection, and non-repudiation; shows how counter-examples may be transferred from one protocol to another using derivation steps; and produces some interesting protocols that appear not to have been previously studied in the open literature.

1 Introduction

Many network protocols with security objectives are designed using a smaller set of common protocol concepts, such as challenge-response, Diffie-Hellman-like key agreement, and "cookies" to reduce potential denial of service. In previous work [5, 6, 7], we proposed a protocol derivation framework based on the use of composition, refinement, and transformation. In this framework, a protocol designer may choose two initial protocol components, refine each of them, compose the results to get a candidate protocol, then apply one or more transformations to improve efficiency or resist particular forms of attack. Ideally, we would like each such derivation to induce an associated security proof, with the security property and its proof determined by the choice of derivation steps. For example, if the last step is a transformation intended to resist denial of service, then we would like to establish, once and for all, that for any protocol (at least if definable within the framework) and for any security property (at least if expressible within the framework), the protocol produced by the transformation has the same security property as the initial protocol, plus a specified denial-of-service property provided by the transformation. This paper takes several

steps toward this long-term goal, presenting a formal treatment of refinement, extending our previous logic with higher-order features to define protocol templates and reason about their instances, extending the logic with symmetric encryption and cryptographic hash functions, and presenting illustrative parts of some case studies.

Composition combines separate protocols, refinements change the content or structure of individual messages, and transformations alter the structure of a protocol. For example, sequential composition places messages of one protocol after messages from the other. In our formal logic, we may prove properties about a composed protocol from its parts, using a set of composition inference rules [6, 7]. The composition rules involve local reasoning about steps in each role and global reasoning about invariants in the protocol or set of protocols in use. In a protocol refinement, a message or portion of a message is systematically refined by, for example, adding additional data or otherwise changing the data contained in one or more messages. For example, replacing a plaintext nonce by an encrypted nonce, in both the sending and receiving protocol roles, is a protocol refinement. While refinements seem to arise naturally in contemporary practical protocols [1, 15], they provide more of a challenge for formal reasoning. One reason is that refinements may involve replacement, and replacement of one term by another does not have a clean formulation in standard mathematical logic.

Adapting concepts from standard higher-logic, we extend our protocol logic by adding function variables and function substitution. This enables us to develop a method for reasoning about protocol refinements. The main idea is to regard a protocol as an instance of a protocol template that is expressed using function variables in place of specific combination of cryptographic or other operations. After proving properties of the protocol template from hypotheses about function variables, we can instantiate the properties and their proofs using different substitutions that respect the hypotheses.

One way of relating abstraction and instantiation to refinement is to consider the proof of a property of a protocol containing messages that use, for example, symmetric encryption. Suppose that this protocol property is preserved if we replace symmetric encryption by use of a keyed hash. Then if we start with a proof of the protocol property that contains symmetric encryption, some branches of the proof tree will establish properties of symmetric encryption that are used in the proof. If we replace symmetric encryption by a function variable, then the protocol proof can be used to produce a proof of the template containing function variables. This is accomplished by replacing each branch that proves a property of symmetric encryption by a corresponding hypothesis about the function variable. Once we have a proof for the protocol template obtained by abstracting away the specific use of symmetric encryption, we can consider replacing the function variable with keyed hash. If keyed hash has the properties of symmetric encryption that were used in the initial proof, we can use proofs of these properties of keyed hash in place of the assumptions about the function variable. Thus an abstraction step and an instantiation step bring us both from a protocol with symmetric encryption to a protocol with keyed hash, and from a proof of the initial protocol to a proof of the final one. The role of the protocol template in this process is to provide a unified proof that leads from shared properties of two primitives (symmetric encryption or keyed hash) to a protocol property that holds with either primitive.

After describing the formal framework, we illustrate the use of protocol templates with several examples. As an example of multiple instantiations of a single template, we prove an authentication property of a generic challenge-response protocol, and then show how to instantiate the template to ISO-9798-2, ISO-9798-3, or SKID3 . As an example of one protocol that is an instance of two templates, we show how to reason about an identity-protection refinement using an authentication template and an encryption template. The third example compares two authentication protocol templates, one that can be instantiated to the ISO-9798 family of protocols, and one that can be

instantiated to STS and SIGMA. The first reflects the authentication mechanism used in JFKi, while the second corresponds to IKE, JFKr, and IKEv2 authentication. While there has been considerable debate and discussion in the IETF community about the tradeoffs offered by these two protocols, previous analyses are relatively low-level and do not illustrate the design principles involved. However, it is possible to compare the authentication properties of the two approaches by comparing the templates.

While our past work on protocol derivation has given rational reconstructions of known protocols, we can also use protocol derivation to combine known protocols in new ways. We begin with two separate derivations. The first, within the JFK family, starts with Diffie-Hellman key exchange protocol and a basic three-step challenge-response protocol. These two are combined to form Station-to-Station (STS), whose key secrecy is based on Diffie-Hellman and authentication property is based on challenge-response. A few steps from STS bring us to a form of JFK. An orthogonal derivation begins with Diffie-Hellman and modifies the functions used, through MTI/A [19] and UM [3] to reach MQV [16]. These two protocol derivations provide a two-dimensional matrix of protocols that have not been explored, to our knowledge. The most sophisticated is a form of JFK using MQV in place of Diffie-Hellman as its key-exchange component. This protocol provides forms of key secrecy, mutual authentication, forward secrecy, known-key security, computational efficiency, identity protection, and denial-of-service protection, inheriting these qualities from protocol design patterns used to produce the protocol.

2 Background

2.1 Derivation System

In [5], we outlined an protocol derivation framework and formalized a subset of it. The framework involves of a set of basic building blocks called *components* and a set of operations for constructing new protocols from old ones. These operations were divided into three general types: *composition*, *refinement*, and *transformation*. As mentioned in the introduction, composition combines separate protocols, refinement change the content or structure of individual messages, and transformation alters the structure of a protocol. Some example components, composition operations, refinements and transformations were described but not fully formalized in [5]. Further examples and more comprehensive formalization of protocol composition appear in [7, 6].

So far, the protocol derivation framework consists of some informal protocol operations, a precise notation for defining protocols, a formal logic for proving properties of protocols, and some connections between the derivation operations and formal proofs. In subsections 2.2 and 2.3, we briefly review the protocol notation and formal logic. Subsection 2.4 contains a short explanation of how we extend both with concepts from higher-order logic in order to support the abstraction-instantiation method that is the focus of this paper.

2.2 Cord Calculus

One important part of security analysis involves understanding the way honest agents running a protocol will respond to messages from a malicious attacker. The common informal arrows-and-messages notation is therefore insufficient, since it only presents the intended executions (or traces) of the protocol. In addition, our protocol logic requires more information about a protocol than the set of protocol executions obtained from honest and malicious parties; we need a high-level description of the program executed by each agent performing each protocol role. As explained in [12], we used a form of process calculus that we call *cords*.

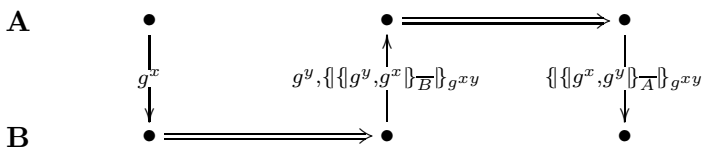

Figure 1: STS as arrows-and-messages

$$\mathbf{A} = [\quad (\nu x) \quad \langle \hat{A}, \hat{B}, g^x \rangle \quad (\hat{B}, \hat{A}, m, \{\!|\{\!|m, g^x|\!\}_B|\!\}_{m^x}) \quad \langle \hat{A}, \hat{B}, \{\!|\{\!|g^x, m|\!\}_{\overline{A}}|\!\}_{m^x} \rangle \quad]$$

$$\mathbf{B} = [\quad (\hat{X}, \hat{B}, n) \quad (\nu y) \quad \langle \hat{B}, \hat{X}, g^y, \{\!|\{\!|g^y, n|\!\}_{\overline{B}}|\!\}_{n^y} \rangle \quad (\hat{X}, \hat{B}, \{\!|\{\!|n, g^y|\!\}_{\overline{X}}|\!\}_{n^y}) \quad]$$

Figure 2: STS as a cord space

The STS protocol is shown in an informal notation in Figure 1 and written as a pair of cords, one for each role, in Figure 2. The arrows between the cords are used in the figure to show how messages sent by one role may be received by the other, but they are not part of the cord formalism. The sequence of actions in the initiator role is given by the cord **A**. The notations (νx), $\langle t \rangle$, (x) refer respectively to the actions of nonce generation, sending a term, and receiving a message. A message is assumed to have the form: (source, destination, content).

In words, the actions of **A** are: generate a fresh nonce; send a message using that number to$\hat{B}$; receive a message with source address $\hat{B}$; verify aspects of the message; and finally, send another message containing date received and the initial nonce generated at the start of the run.

2.3 A Protocol Logic

Our basic protocol logic and proof system are developed in [12, 5, 7, 6], with [7] providing a relatively succinct presentation of the most recent form. A brief summary is also included in Appendix A.

The formulas of the logic are given by the grammar in Table 1, where ρ may be any role, written using the notation of cord calculus. Here, t and P denote a term and a process respectively. We use the word *process* to refer to a principal executing an instance of a role. As a notational convention, we use X to refer to a process belonging to principal $\hat{X}$. We use ϕ and ψ to indicate predicate formulas, and m to indicate a generic term we call a "message".

Most protocol proofs use formulas of the form $\theta[P]_X\phi$, which means that after actions P are executed in process X, starting from a state where formula θ is true, formula ϕ is true about the resulting state of X. Here are the informal interpretations of the predicates (see [7] for detailed semantics):

$\mathsf{Has}(X, x)$ means principal $\hat{X}$ possesses information x in the process X. This is "posses" in the limited sense of having either generated the data or received it in the clear or received it under encryption where the decryption key is known.

$\mathsf{Send}(X, m)$ means principal $\hat{X}$ sends message m in the process X.

$\mathsf{Receive}(X, m)$, $\mathsf{New}(X, t)$, $\mathsf{Decrypt}(X, t)$, $\mathsf{Verify}(X, t)$ similarly mean that receive, new, decrypt and signature verification actions occur.

Action formulas
$\mathsf{a} \quad ::= \quad \mathsf{Send}(P,m) \mid \mathsf{Receive}(P,m) \mid \mathsf{New}(P,t) \mid \mathsf{Decrypt}(P,t) \mid \mathsf{Verify}(P,t)$
Formulas
$\phi \quad ::= \quad \mathsf{a} \mid \mathsf{Has}(P,t) \mid \mathsf{Fresh}(P,t) \mid \mathsf{Honest}(N) \mid \mathsf{Contains}(t_1,t_2) \mid \phi \wedge \phi \mid \neg\phi \mid \exists x.\phi \mid \diamondminus \phi \mid \ominus \phi$
Modal forms
$\Psi \quad ::= \quad \rho\ \phi \mid \phi\ \rho\ \phi$

Table 1: Syntax of the logic

$\mathsf{Fresh}(X,t)$ the term t generated in X is "fresh" in the sense that no one else has seen any term containing t as a subterm. Typically, a fresh term will be a nonce and freshness will be used to reason about the temporal ordering of actions in runs of a protocol.

$\mathsf{Honest}(\hat{X})$ the actions of principal $\hat{X}$ in the current run are precisely an interleaving of initial segments of traces of a set of roles of the protocol. In other words, $\hat{X}$ assumes some set of roles and does exactly the actions prescribed by them.

The two temporal operators $\diamondminus$ and $\ominus$ have the same meaning as in Linear Temporal Logic [18]. Since we view a run as a linear sequence of states, $\diamondminus\ \phi$ means that in some state in the past ϕ holds, whereas $\ominus\ \phi$ means that in the previous state ϕ holds.

The predicate $\mathsf{After}(\mathsf{a}_1, \mathsf{a}_2)$, definable from $\diamondminus$ and $\ominus$, means that the action a_2 happened after the action a_1 in a run. Other predicates such as Computes and Contains are also definable in the logic.

2.4 Cords and Protocol Logic with Function Variables

Like a program module containing functions that are not defined in the module, a cord may contain functions that are not given a specific meaning in the cord calculus. When a cord contains undefined functions, the cord cannot be executed as is, but can be used to define a set of runs if the function is replaced by a combination of defined operations. Since cords contain functions such as encryption and pairing, it is a simple matter to extend the syntax with additional function names. Since we will apply substitution for these function names, and implicitly quantify over their possible interpretations in the protocol logic, we refer to these function names as function variables. The mechanism for substituting an expression for a function variable, in a manner that treats function arguments correctly, is standard in higher-order logic. A simple explanation that does not involve lambda calculus or related machinery is given at the beginning of [13], for example.

In a judgement

$$\mathcal{Q}, \Gamma \vdash \phi_1 [P]_A \phi_2$$

where $\mathcal{Q}$ is a protocol containing function variables, P is one role or initial segment of a role of the protocol, and Γ denotes the set of assumed properties and invariants, the formulas in Γ may also contain function variables. The meaning of this judgement is that for every substitution that eliminates all function variables, any execution of the resulting protocol $\mathcal{Q}'$ respecting the resulting invariants Γ', the resulting formula $\phi_1' [P']_A \phi_2'$ holds. It is straightforward to show that our previous logic is sound for protocols and assertions containing function variables, and that substitution preserves semantic entailment and validity of formulas.

As a technical note for logicians, we observe that since we do not have any comprehension principle for our logic, it is actually reducible to first-order logic by the standard method of treating function variables as first-order variables via an Apply function. Consequently, our higher-order protocol logic is no less tractable (for automated theorem proving) than the logic without function variables. Consequently, our higher-order protocol logic is no less tractable (for automated theorem proving) than the logic without function variables.

3 Abstraction and Refinement Methodology

Protocol Templates: A *protocol template* is a protocol that uses function variables. An example of an abstract challenge-response based authentication protocol using the informal trace notation is given below.

$$\begin{array}{l} A \rightarrow B : m \\ B \rightarrow A : n, F\,(B, A, n, m) \\ A \rightarrow B : G\,(A, B, m, n) \end{array}$$

Here, m and n are fresh nonces and F and G are function variables. Substituting cryptographic functions for F and G with the parameters appropriately filled in yields real protocols. For example, instantiating F and G to signatures yields the standard signature-based challenge-response protocol from the ISO-9798-3 family, whereas instantiating F and G to a keyed hash yields the SKID3 protocol.

Characterizing protocol concepts: Protocol templates provide a useful method for formally characterizing design concepts. Our methodology for formal proofs involves the following two steps.

1. Assuming properties of the function variables and some invariants, prove properties of the protocol templates. Formally,

   $$\mathcal{Q}, \Gamma \vdash \phi_1[P]_A\phi_2$$

   Here, $\mathcal{Q}$ is an abstract protocol and P is a program for one role of the protocol. Γ denotes the set of assumed properties and invariants.

2. Instantiate the function variables to cryptographic functions and prove that the assumed properties and invariants are satisfied by the real protocol. Hence conclude that the real protocol possesses the security property characterized by the protocol templates.

   $$If\ \mathcal{Q}' \vdash \Gamma',\ then\ \mathcal{Q}' \vdash \phi_1'[P']_A\phi_2'$$

   Here, the primed versions of the protocol, hypotheses, etc. are obtained by applying the substitution σ used in the instantiation.

The correctness of the method follows from the soundness of substitution and the transitivity of entailment in the logic, as described in Section 2.4.

Combining protocol templates: Protocol templates can also be used to formalize the informal practice of protocol design by combining different mechanisms. The key observation is that if a concrete protocol is an instantiation of two different protocol templates, each instantiation respecting the assumed invariants associated with the template, then the concrete protocol has the security properties of both templates. Our methodology involves the following three steps.

1. Identify two protocol templates which guarantee certain security properties under some assumptions.

$$\mathcal{Q}_1, \Gamma_1 \vdash \phi_{11}[P_1]_A\phi_{21} \quad and \quad \mathcal{Q}_2, \Gamma_2 \vdash \phi_{12}[P_2]_A\phi_{22}$$

   Here, $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are protocol templates; P_1 and P_2 are respectively the programs corresponding to a specific role; and Γ_1 and Γ_2 denote the sets of assumed properties and invariants.

2. Find substitutions σ_1 and σ_2 such that the two instantiated protocols and roles are identical, i.e.,

$$\sigma_1\mathcal{Q}_1 = \sigma_2\mathcal{Q}_2 = \mathcal{Q}' \quad and \quad \sigma_1 P_1 = \sigma_2 P_2 = P'$$

3. Prove that the instantiated protocol satisfies the hypotheses of both the protocol templates. Hence conclude that it inherits the security properties of both.

$$If\ \mathcal{Q}' \vdash \Gamma'_1 \cup \Gamma'_2,\ then\ \mathcal{Q}' \vdash (\phi'_{11} \wedge \phi'_{12})[P']_A(\phi'_{21} \wedge \phi'_{22})$$

   Here, the primed versions of the protocol, hypotheses, etc. are obtained by applying the substitutions σ_1 and σ_2 used in the instantiations.

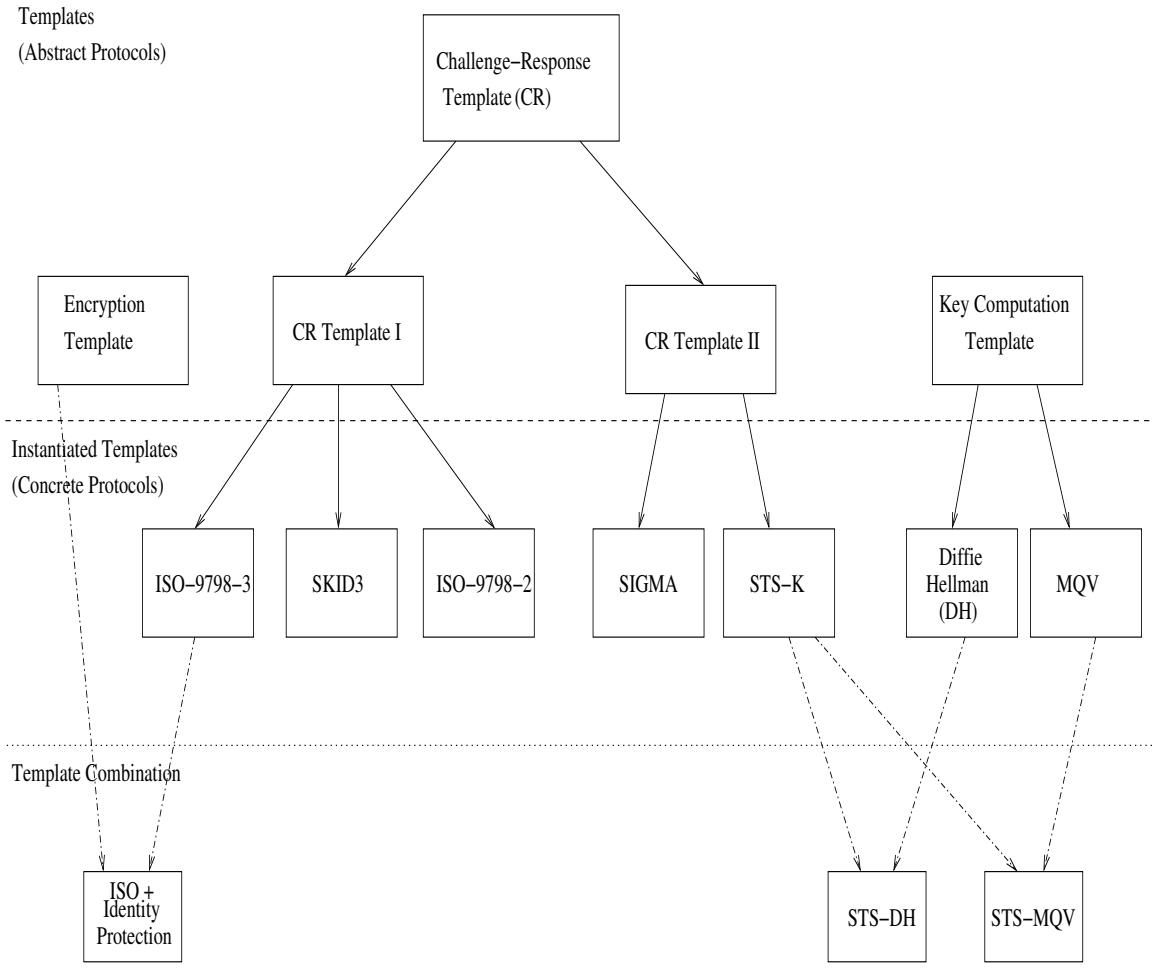

Figure 3: Illustrating the Methodology

4 Illustrative Examples

In the previous section, we introduced the notion of generic protocol templates and presented an abstraction-instantiation methodology for proving properties of related protocols by reusing one general proof pattern. In this section, we present several examples illustrating this methodology. The protocols considered include real world protocols from the ISO and IKE families.

4.1 Characterizing Protocol Templates

A generic protocol template can be instantiated to multiple real protocols. Identifying such templates and characterizing the associated security properties under assumed hypotheses is useful for several reasons. Such characterizations underpin basic principles used in designing classes of protocols and bring out subtle tradeoffs offered by various protocol families (see Section 4.3 for an interesting example). Another obvious benefit is that the security proofs of instances of a template follow from the proof of the template plus a (usually much simpler) proof that the instances satisfy the assumed hypotheses. In what follows, we work through an example demonstrating the approach.

4.1.1 Example: Challenge-Response Template

In our first example, we characterize a generic challenge-response protocol template and then obtain three real protocols: ISO-9798-2, ISO-9798-3, and SKID3 by appropriate substitutions. In doing so, we follow the two step methodology outlined in Section 3.

Step 1: The first step is to precisely define and characterize the abstract protocol. This involves defining the abstract protocol (denoted Q_{CR} in the sequel) as a cord space, expressing the security property achieved, and identifying the set of assumptions under which the property holds. The programs for the initiator and responder roles of Q_{CR} is written out below in the notation of cords.

$$\begin{aligned}\mathbf{Init_{CR}} &= (\nu n)\ (\{\hat{A}, \hat{B}, m, \})\ \langle\{\hat{B}, \hat{A}, n, F(\hat{B}, \hat{A}, n, m)\}\rangle\ (\{\hat{A}, \hat{B}, G(\hat{A}, \hat{B}, m, n)\}) \\ \mathbf{Resp_{CR}} &= \langle\{\hat{Y}, \hat{B}, y\}\rangle\ (\nu n)\ (\{\hat{B}, \hat{Y}, n, F(\hat{B}, \hat{Y}, n, y)\})\ \langle\{\hat{Y}, \hat{B}, G(\hat{Y}, \hat{B}, y, n)\}\rangle\end{aligned}$$

Here, F and G are function variables. Under a set of assumptions (Γ_{CR}) about these variables, we prove an authentication property of the protocol using the logic (see Table 4 in Appendix B for the complete formal proof).

$$Q_{CR}, \Gamma_{CR} \vdash [\mathbf{Init_{CR}}]_A\ \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(B) \supset \phi_{auth}$$

Intuitively, this formula means that if A executed a session of Q_{CR} supposedly with B and both of them are honest (implying that they strictly follow the protocol and do not, for example, send out their private keys), then the authentication property expressed by the formula ϕ_{auth} holds in the resulting state. ϕ_{auth} specifies an authentication property for the initiator based on the concept of *matching conversations* [9]. Simply put, it requires that whenever A completes a session supposedly with B, both A and B have consistent views of the run, i.e., they agree on the content and order of the messages exchanged. Formally,

$$\begin{aligned}\phi_{auth} \equiv\ & \exists B.(\mathsf{ActionsInOrder}(\\ & \mathsf{Send}(A, \{\hat{A}, \hat{B}, m, \}), \mathsf{Receive}(B, \{\hat{A}, \hat{B}, m, \}), \\ & \mathsf{Send}(B, \{\hat{B}, \hat{A}, n, F(\hat{B}, \hat{A}, n, m)\}), \mathsf{Receive}(A, \{\hat{B}, \hat{A}, n, F(\hat{B}, \hat{A}, n, m)\}), \\ & \mathsf{Send}(A, \{\hat{A}, \hat{B}, G(\hat{A}, \hat{B}, m, n)\}), \mathsf{Receive}(B, \{\hat{A}, \hat{B}, G(\hat{A}, \hat{B}, m, n)\})))\end{aligned}$$

The set of assumptions Γ_{CR} used to prove the authentication property consists of the following four logical formulas:

$$\begin{aligned}
\gamma_1 &\equiv \mathsf{Computes}(X, F(\hat{B}, \hat{A}, n, m)) \supset (\exists A'.X = A') \vee (\exists B'.X = B') \\
\gamma_2 &\equiv \neg\mathsf{Contains}(\{\hat{X}, \hat{Y}, x\}, F(\hat{B}, \hat{A}, n, m)) \\
\gamma_3 &\equiv \mathsf{Contains}(\{\hat{X}, \hat{Y}, G(\hat{X}, \hat{Y}, x, y)\}, F(\hat{B}, \hat{A}, n, m)) \supset \hat{X} = \hat{B} \wedge \hat{Y} = \hat{A} \wedge n = y \wedge m = x \\
\gamma_4 &\equiv \mathsf{Contains}(\{\hat{X}, \hat{Y}, x, F(\hat{X}, \hat{Y}, x, y)\}, F(\hat{B}, \hat{A}, n, m)) \supset \hat{X} = \hat{B} \wedge \hat{Y} = \hat{A} \wedge n = x \wedge m = y
\end{aligned}$$

Informally, assumption γ_1 states that the function variable F is hard to compute: only agents $\hat{A}$ and $\hat{B}$ can compute $F(\hat{B}, \hat{A}, n, m)$ (more precisely, if some session X has enough information to compute $F(\hat{B}, \hat{A}, n, m)$ then X is either session of agent $\hat{A}$ or agent $\hat{B}$). In a concrete protocol, this assumption can be satisfied by, for example, instantiating F to a signature. The other assumptions impose syntactic constraints on F and G. For example, an γ_2 implies that $F(\hat{B}, \hat{A}, n, m)$ cannot be mistaken for a nonce. This obviates certain type confusion attacks. Formula γ_4 implies that F depends on the value of all four parameters.

A complete proof of the authentication property for the initiator role of the Challenge-Response template is given in Table 4 in Appendix B. Below, we discuss the structure of the proof of the Challenge-Response protocol and provide some insight on the proof technique used to prove authentication results in this logic.

Proof Structure of Challenge-Response Template: The formal proof in Table 4 naturally breaks down into four parts:

- Line (1) asserts what actions were executed by Alice in the initiator role. Specifically, we can conclude that Alice has received a message msg containing $F(\hat{B}, \hat{A}, n, m)$.
- In lines (2)–(9), we track the source of term $F(\hat{B}, \hat{A}, n, m)$ received by Alice. First, since Alice received a message containing $F(\hat{B}, \hat{A}, n, m)$, there must be a process who computed that term and send it on the network. Using the assumption γ_1, we can conclude that only Alice or Bob could have computed $F(\hat{B}, \hat{A}, n, m)$. Finally, using the assumptions $\gamma_2, \gamma_3, \gamma_4$, we can deduce that it is not the case that Alice has send $F(\hat{B}, \hat{A}, n, m)$. Therefore, Bob has send a message msg' containing $F(\hat{B}, \hat{A}, n, m)$.
- In lines (10)–(13), we use the honesty rule, and assumptions $\gamma_2, \gamma_3, \gamma_4$ to conclude that Bob must have sent $F(\hat{B}, \hat{A}, n, m)$ as a part of the second message of the responder role. Therefore, Bob has received a corresponding first message in the past. Also, using γ_4, we can conclude that Bob is in the session with Alice.
- Finally, in lines (14)–(19), the temporal ordering rules are used to establish a total ordering among the send-receive actions of Alice and Bob. Line (17) concludes that Bob must have received msg1 after Alice sent it since msg1 contains a fresh nonce. Line (18) uses the same argument for msg2 sent by Bob. Finally, line (19) uses the transitivity axiom to conclude that the authentication formula ϕ_{auth} is true.

This completes the characterization of the protocol template. We are now ready to move on to Step 2.

$F(X,Y,x,y) \equiv E_{K_{XY}}(x,y,X)$	$F(X,Y,x,y) \equiv H_{K_{XY}}(x,y,X)$	$F(X,Y,x,y) \equiv SIG_X(x,y,Y)$
$G(X,Y,x,y) \equiv E_{K_{XY}}(y,x)$	$G(X,Y,x,y) \equiv H_{K_{XY}}(y,x,X)$	$G(X,Y,x,y) \equiv SIG_X(y,x,Y)$
$A \to B : m$	$A \to B : m$	$A \to B : m$
$B \to A : n, E_{K_{AB}}(n,m,B)$	$B \to A : n, H_{K_{AB}}(n,m,B)$	$B \to A : n, SIG_B(n,m,A)$
$A \to B : E_{K_{AB}}(n,m)$	$A \to B : H_{K_{AB}}(n,m,A)$	$A \to B : SIG_A(n,m,B)$
ISO 9798-2	SKID3	ISO 9798-3

Figure 4: Instantiations of the Challenge-Response template

Step 2: In this step, we instantiate the protocol template to three well known protocols from the ISO family. The substitutions for the function variables and the resulting protocols are shown in Figure 4. ISO 9798-2, SKID3, and ISO 9798-3 [21] respectively use symmetric key encryption with a pre-shared key, keyed hash and signatures to instantiate F and G. These substitutions respect the assumed invariants in Γ_{CR}. (For example, γ_1 is satisfied by signatures since the signature can be computed only by an agent who has the corresponding private key. The formal proofs follow immediately from logical axioms and are omitted.) We can therefore conclude that all three protocols guarantee the authentication property characterized by the abstract protocol.

4.2 Combining Protocol Templates

A refinement operation (as defined in [5]), when applied to a protocol, adds an additional security property while preserving the original properties. Examples of refinement operations considered in [5] include replacing signatures by encrypted signatures to provide identity protection and replacing fresh Diffie-Hellman exponentials by a pair consisting of a stale exponential and a fresh nonce, thereby enabling reuse of exponentials and hence greater computational efficiency. The methodology for combining protocol templates, described in Section 3, provides a way to formally reason about a broad class of refinements including the two just mentioned. Below we illustrate the general method by examining the identity protection refinement in some detail.

4.2.1 Example: Identity Protection Refinement

In this example, we start with a signature based protocol, ISO-9798-3, that provides mutual authentication. We apply the identity protection refinement to it, which involves replacing the signatures by encrypted signatures using a shared key. (The intention is to prevent adversaries from observing signatures since they can reveal identities of communicating peers.) The goal is to prove that this refinement step is correct, i.e., it does indeed guarantee that the resulting protocol provides identity protection, while preserving the mutual authentication property of the original protocol. We identify two templates: Q_{CR}, the challenge-response template described in the previous section, and Q_{ENC} described below, which provides a form of secrecy. The aim now is to prove that the protocol obtained after the refinement step is an invariant respecting instance of both these patterns and the terms protected by the secrecy pattern are precisely the signatures.

Step 1: The Q_{CR} template has been defined and characterized in an earlier section. Here, we do the same for the Q_{ENC} template. Using the informal arrows-and-messages diagram, the template

can be described as follows.

$$A \to B : m$$
$$B \to A : n, E_{K_{AB}}(H(B, A, n, m))$$
$$A \to B : E_{K_{AB}}(I(A, B, m, n))$$

The programs for the initiator and responder roles of Q_{ENC} is written out below in the notation of cords.

$$\mathbf{Init_{ENC}} = (\nu m)\ (\{\hat{A}, \hat{B}, m\})\ \langle\{\hat{B}, \hat{A}, n, E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m))\}\rangle\ (\{\hat{A}, \hat{B}, E_{K_{AB}}(I(\hat{A}, \hat{B}, m, n))\})$$
$$\mathbf{Resp_{ENC}} = \langle\{\hat{Y}, \hat{B}, y\}\rangle\ (\nu n)\ (\{\hat{B}, \hat{Y}, n, E_{K_{BY}}(H(\hat{B}, \hat{Y}, n, y))\})\ \langle\{\hat{Y}, \hat{B}, E_{K_{BY}}(I(\hat{Y}, \hat{B}, y, n))\}\rangle$$

Here, H and I are function variables. Under a set of assumptions (Γ_{ENC}) about these variables, we prove that the term $H(\hat{B}, \hat{A}, n, m)$ remains secret: it is known only to A and B (see Table 5 in Appendix A for a detailed proof). Formally,

$$Q_{ENC}, \Gamma_{ENC} \vdash [\mathbf{Init_{ENC}}]_A\ \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(B) \supset \phi_{secret}$$

Intuitively, this formula means that if A executed a session of Q_{ENC} supposedly with B and both of them are honest (implying that they strictly follow the protocol and do not, for example, send out their private keys), then the secrecy property expressed by the formula ϕ_{secret} holds in the resulting state. ϕ_{secret} specifies the secrecy property for the term $H(\hat{B}, \hat{A}, n, m)$. Formally,

$$\phi_{secret} \equiv \exists B.(\mathsf{Has}(X, H(\hat{B}, \hat{A}, n, m)) \supset X = A \vee X = B)$$

The set of assumptions Γ_{ENC} used to prove the authentication property consists of the following four logical formulas:

$$\delta_1 \equiv \mathsf{Computes}(X, H(\hat{B}, \hat{A}, n, m)) \supset \exists B.X = B$$
$$\delta_2 \equiv \neg\mathsf{Contains}(\{\hat{X}, \hat{Y}, x\}, H(\hat{B}, \hat{A}, n, m))$$
$$\delta_3 \equiv \mathsf{Contains}(\{\hat{X}, \hat{Y}, E_{K_{XY}}(I(\hat{X}, \hat{Y}, x, y))\}, H(\hat{B}, \hat{A}, n, m)) \supset \hat{X} = \hat{B} \wedge n = y \wedge m = x$$
$$\delta_4 \equiv \mathsf{Contains}(\{\hat{X}, \hat{Y}, x, E_{K_{XY}}(H(\hat{X}, \hat{Y}, x, y))\}, H(\hat{B}, \hat{A}, n, m)) \supset \hat{X} = \hat{B} \wedge n = x \wedge m = y$$

These formulas capture simple ideas, e.g., $H(\hat{B}, \hat{A}, n, m)$ (e.g. $B's$ signature) can be computed only by B and certain syntactic constraints, e.g., a signature is not a subterm of a nonce.

$F(X, Y, x, y) \equiv E_{K_{XY}}(SIG_X(x, y))$	$A \to B : m$	$H(X, Y, x, y) \equiv SIG_X(x, y)$
$G(X, Y, x, y) \equiv E_{K_{XY}}(SIG_X(y, x))$	$B \to A : n, E_{K_{AB}}(SIG_B(n, m))$	$I(X, Y, x, y) \equiv SIG_X(y, x)$
CR	$A \to B : E_{K_{AB}}(SIG_A(n, m)))$	

Figure 5: Protocol that is an instantiation of both CR and ENC patterns

Step 2: The second step is to find substitutions σ_1 and σ_2 such that both the templates (Q_{CR} and Q_{ENC}) instantiate to the same real protocol. The desired substitutions are shown in Figure 5. σ_1 is on the left, σ_2 is on the right and the instantiated protocol is in the middle of the figure.

Step 3: The final step is to verify that the instantiated protocol satisfies the union of the hypotheses in Γ_{CR} and Γ_{ENC}. This follows easily from the properties of signature and encryption under symmetric key as expressed in the logic and the syntactic structure of the protocol. We can therefore conclude that the identity protection refinement operation as applied here is correct, i.e., it adds the identity protection property while preserving the original properties of the protocol (which in this case is mutual authentication).

4.3 Authenticated Key-Exchange Templates

An important use of protocol templates is to underpin basic principles used in designing classes of protocols and to bring out subtle tradeoffs offered by various protocol families. In this section, we examine two families of authenticated key exchange protocols. The first template, $AKE1$, generalizes a family of protocols in which authentication is achieved by explicitly embedding the intended recipient's identity inside authenticators in messages. This family includes the ISO-9783-3 key exchange protocol and related protocols including the core JFKi protocol. The second template, $AKE2$, generalizes a family of protocols where agents authenticate each other using a combination of signatures and a proof of possession of the Diffie-Hellman shared secret computed during the execution of the protocol. This family includes, STS, SIGMA, and the core of the IKE and JFKr protocols. Part of the reason these two families are interesting is that they were both candidates for the recently proposed IKEv2 protocol and there has been considerable discussion and debate in the IETF community about the tradeoffs offered by the two designs. The use of templates to characterize the two families sheds light on the subtle difference between the authentication and identity protection guarantees associated with the two sets of protocols.

Template AKE1: Using the informal arrows-and-messages diagram, the authenticated key-exchange template AKE1 can be described as follows.

$$\begin{array}{l} A \rightarrow B : A, g^a \\ B \rightarrow A : g^b, F(B, A, g^b, g^a) \\ A \rightarrow B : G(A, B, g^a, g^b) \end{array}$$

For this template, we are able to prove both secrecy and authentication for the initiator role:

$$Q_{AKE1}, \Gamma_{AKE1} \vdash [\mathbf{Init_{AKE1}}]_A \; \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(B) \supset \phi_{auth} \wedge \phi_{shared-secret}$$

The formula ϕ_{auth} describes an authentication property for the initiator based on matching conversations, while formula $\phi_{shared-secret}$ states that A and B the the only two sessions which know the Diffie-Hellman secret g^{ab}. The set of assumptions Γ_{AKE1} is similar to Γ_{CR} in Section 4.1.1:

$$\begin{array}{lcl} \epsilon_1 & \equiv & \mathsf{Computes}(X, F(\hat{B}, \hat{A}, g^b, g^a)) \supset \exists B'.X = B' \\ \epsilon_2 & \equiv & \neg\mathsf{Contains}(\{\hat{X}, \hat{Y}, g^x\}, F(\hat{B}, \hat{A}, g^b, g^a)) \\ \epsilon_3 & \equiv & \mathsf{Contains}(\{\hat{X}, \hat{Y}, G(\hat{X}, \hat{Y}, g^x, g^y)\}, F(\hat{B}, \hat{A}, g^b, g^a)) \supset \hat{X} = \hat{B} \wedge \hat{Y} = \hat{A} \wedge g^b = g^y \wedge g^a = g^x \\ \epsilon_4 & \equiv & \mathsf{Contains}(\{\hat{X}, \hat{Y}, g^y, F(\hat{X}, \hat{Y}, g^x, g^y)\}, F(\hat{B}, \hat{A}, g^b, g^a)) \supset \hat{X} = \hat{B} \wedge \hat{Y} = \hat{A} \wedge g^b = g^x \wedge g^a = g^y \end{array}$$

We prove that the ISO-9798-3 key exchange protocol satisfies the set of assumptions, Γ_{AKE1}, and therefore provides similar authentication and secrecy guarantees. However, STS, SIGMA and their variants do not satisfy Γ_{AKE1}. Specifically, the assumption ϵ_4 fails since the intended recipient's identity is not embedded in the second message of the protocol. The way the proof fails leads us to an run which provides a counterexample to the strong authentication property. This works for both STS and SIGMA and the run is essentially similar to the "attack" on STS first demonstrated by Lowe in [17].

Template AKE2: Using the informal arrows-and-messages diagram, AKE2 can be described as follows.

$$\begin{array}{l} A \rightarrow B : g^a \\ B \rightarrow A : g^b, F(B, g^b, g^a), F'(B, g^{ab}) \\ A \rightarrow B : G(A, g^a, g^b), G'(A, g^{ab}) \end{array}$$

$A \to B : g^a$	$A \to B : g^a$	$A \to B : g^a$
$B \to A : g^b, SIG_B(g^b, g^a, A)$	$B \to A : g^b, E_{g^{ab}}(SIG_B(g^a, g^b))$	$B \to A : g^b, SIG_B(g^b, g^a), H_{g^{ab}}(B)$
$A \to B : SIG_A(g^a, g^b, B)$	$A \to B : E_{g^{ab}}(SIG_A(g^b, g^a))$	$A \to B : SIG_A(g^b, g^a), H_{g^{ab}}(A)$
ISO 9798-3 Key exchange	STS	Basic SIGMA

Figure 6: Instantiations of Authenticated Key-Exchange Templates

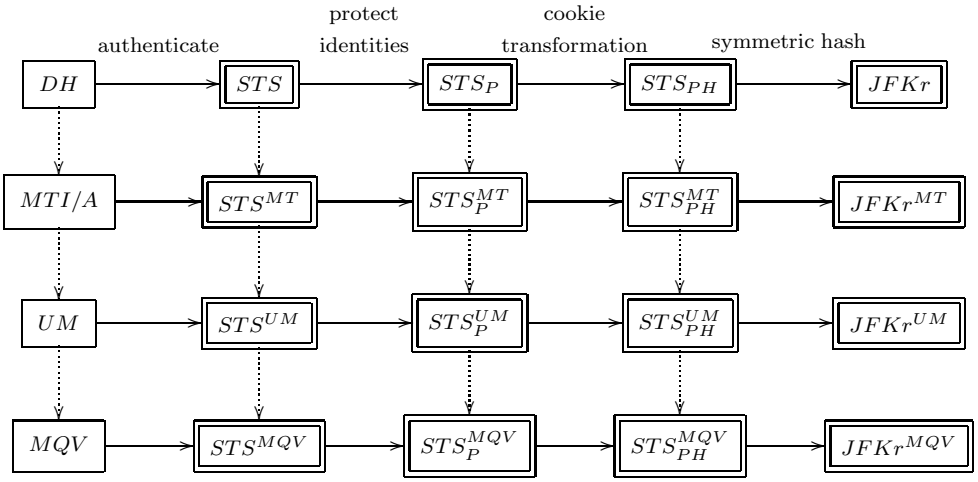

Figure 7: Design by Combining Templates

Informally, the purpose of F is to ensure that B is a session with parameters g^a and g^b, while F' proves that B has the shared secret g^{ab}. Combining the two facts derived from certain assumptions about the function variables, it is possible to prove that this protocol template provides a form of authentication: matching conversations for the responder. However, as mentioned before, this protocol does not have the matching conversations based authentication property for the initiator. It therefore follows that the class of protocols characterized by the AKE1 template provide stronger authentication guarantees than the class characterized by AKE2.

5 Deriving the STS-MQV Protocol Family

While previous sections have focussed on formal reconstruction of known protocols, here we examine the possibility of synthesizing new protocols by reusing constructs from existing protocols. We begin with two well-known protocol families: the first includes Diffie-Hellman key exchange and several variants that enhance the key derivation function (MTI/A, UM and MQV); the second is the IKE family - STS being the base protocol and a few steps further on is JFKr. These two protocol families are combined to map out a two-dimensional matrix of protocols (see Figure 5) which, to the best of our knowledge, has not been previously studied in the open literature. An intuitive presentation of this derivation is in Appendix C. The focus here is on a core part of the synthesis that follows naturally from the abstraction and refinement methodology. Specifically, we formally prove properties of the protocols in the first three columns of Figure 5, while the derivation steps involved in going to the next two columns are not yet formalized, although we believe that they can be handled by simple extensions of the current logic.

5.1 Formal Synthesis

We identify two base protocol templates: a key computation template (KC) and an authenticated key exchange template (AKC). AKC relies on a key computation template with exactly the properties characterized by KC. The first column in Figure 5 contains protocols DH, MTI/A, UM and MQV which are instantiations of KC; the second column has instantiations of AKC, where each instantiated protocol uses the KC instantiation on its left (e.g., STS^{MQV} uses MQV). In Section 5.2, we prove the security properties of these protocols using the abstraction and instantiation methodology. The protocols in the third column are obtained from those in the second by applying an identity protection refinement. Formally, this involves combining the AKC template with an encryption template in a manner similar to Example 4.2.1 in Section 4.2. The proofs are omitted due to space constraints. The subsequent steps in the derivation involve protocol transformations not formalized currently. We hope to address this issue in future work as part of a larger effort to develop a general theory of protocol transformations.

5.2 Characterizing and Combining KC and AKC

In this section, we discuss the main ideas used in characterizing and combining the KC and AKC templates. Detailed proofs are omitted due to space constraints.

Key Computation Template, KC. The template is characterized by a formula capturing the idea that a shared key has associated with it two public-private key pairs and in order to compute the key, it is necessary and sufficient to possess one private key and the other public key. Formally,

$$\mathsf{Computes}(X, H(t_1, f(t_1), t_2, f(t_2))) \equiv \mathsf{Has}(X, (t_1, f(t_2))) \vee \mathsf{Has}(X, (t_2, f(t_1)))$$

Here, H is a function variable denoting the key computation function while the variable f denotes the function that is used to compute the public key given the private key. It is easy to see that the key computation functions of all four protocols (DH through MQV) satisfy this hypothesis. For example, the Diffie-Hellman shared key g^{ab} is associated with the public-private key pairs (g^a, a) and (g^b, b) and computing it requires either (a, g^b) or (b, g^a). Similarly, computing the UM key requires either $((a, x), (g^b, g^y))$ or $((b, y), (g^a, g^x))$, where the public-private key pairs are $((g^a, g^x), (a, x))$ and $((g^b, g^y), (b, y))$. Note that the hypothesis for this template only characterizes the properties of certain functions. The proof that a particular instantiation has this property must therefore follow from axioms of the proof system and is independent of the protocol in which this template is used. This observation will be crucial when subsequently we combine this template with AKC.

Authenticated Key Exchange Template, AKC. AKC (given below) is a generalization of AKE2, the template which yielded STS and SIGMA in Section 4.3. The further abstraction step arises from understanding that the essential property provided by the Diffie-Hellman terms is characterized by the KC template. In particular, AKE2 can be obtained by instantiating the function variables f and H to the Diffie-Hellman functions.

$$\begin{aligned}
&A \to B : f(t_1) \\
&B \to A : f(t_2), F(B, f(t_1), f(t_2)), F'(B, H(t_1, f(t_1), t_2, f(t_2))) \\
&A \to B : G(A, f(t_2), f(t_1)), G'(A, H(t_1, f(t_1), t_2, f(t_2)))
\end{aligned}$$

The invariants characterizating this template are similar to those for AKE2, the only difference being that function variables replace actual Diffie-Hellman functions and the key computation

property of KC is added to the hypothesis set. The formal proof that this abstract protocol provides an authenticated shared secret is exactly the same as the corresponding proof for AKE2 presented earlier.

Combining the Templates Diffie-Hellman and MQV functions are instantiations of the KC template and, as noted earlier, since this template depends only on the functions, the property is guaranteed irrespective of the message structure of the specific protocol in which they are used. Instantiating the underlying KC template of AKC with Diffie-Hellman and using encrypted signatures over public keys gives us the STS protocol. As proved in Section 4.3, this protocol satisfies the assumed invariants of AKE2 and hence AKC. It therefore provides an authenticated shared secret.

$$
\begin{array}{l}
A \rightarrow B : g^x \\
B \rightarrow A : g^y, C_B, E_K\left(SIG_B(g^y, g^x)\right) \\
A \rightarrow B : C_A, E_K\left(SIG_A(g^x, g^y)\right)
\end{array}
$$

On the other hand, instantiating the KC template of AKC to MQV and using a combination of certified Diffie-Hellman keys and encryptions over the public keys, we get the new STS^{MQV} protocol. This protocol also satisfies the assumed invariants of the AKC template and therefore guarantees an authenticated shared secret.

$$
\begin{array}{l}
A \rightarrow B : g^x, g^a \\
B \rightarrow A : g^y, g^b, G_B, E_K\left(g^y, g^x\right) \\
A \rightarrow B : G_A, E_K\left(g^x, g^y\right)
\end{array}
$$

An advantage of this protocol over STS is that it is computationally more efficient, a property that it inherits from the MQV protocol (see Appendix C for further discussion).

6 Conclusions and Future Work

While there is ample evidence that protocol designers think systematically about protocol requirements and the means to achieve them (e.g., [2, 15]), it is a significant challenge to make these natural intuitions precise enough to provide systematic proofs of protocol properties. We believe that protocol templates, and an accompanying higher-order extension or our previous protocol logic, furnish some useful techniques for modular reasoning. In particular, similar protocols can now be proved to have identical or related properties using a single proof about a protocol template. Moreover, it is possible for multiple properties of a single protocol to be established using different templates for each property. While we have illustrated these general protocol proof methods with a few simple examples, we believe that many more templates and associated proofs can be devised.

The logical foundation for the proof method shown in this paper is the very simple idea of extending a protocol notation (cords) and protocol logic with function variables. This allows protocol templates to be written in a natural way, and allows them to be proved correct using implicit universal quantification over function variables.

We have developed some challenge-response and key generation protocol templates that also required adding symmetric encryption and cryptographic hash to our previous protocol logic. We also used protocol templates to exploring a design space surrounding JFK (Just Fast Keying) and related protocols from the IKE (Internet Key Exchange) family. This exploration reveals some trade-offs between authentication, identity protection, and non-repudiation; shows how counter-examples may be transferred from one protocol to another using derivation steps; and produces some interesting protocols that appear not to have been previously studied in the open literature.

In future work, we hope to develop useful tool support for protocol derivation steps and the associated logic. A current effort underway draws on program derivation and verification experience at Kestrel Institute. The software infrastructure supporting protocol derivations is based on *especs* [22, 23, 4], a framework for refinement and automated composition of state machines, where states are annotated by algebraic specifications, and transitions by morphisms between them.

References

[1] W. Aiello, S.M. Bellovin, M. Blaze, R. Canetti, A.D. Keromytis J. Ioannidis, and O. Reingold. Just fast keying (JFK), 2002. Internet draft.

[2] William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, and Angelos D. Keromytis. Efficient, dos-resistant, secure key exchange for internet protocols. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 48–58. ACM Press, 2002.

[3] R. Ankney, D. Johnson, and M. Matyas. The unified model, 1995. Contribution to X9F1.

[4] Matthias Anlauf and Dusko Pavlovic. On specification carrying software, its refinement and composition. In H. Ehrig, B.J. Kramer, and A. Ertas, editors, *Proceedings of IDPT 2002*. Society for Design and Process Science, 2002.

[5] A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. A derivation system for security protocols and its logical formalization. In *Proceedings of 16th IEEE Computer Security Foundations Workshop*. IEEE, 2003.

[6] A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. Secure protocol composition. Proceedings of Mathematical Foundations of Programming Semantics, to appear in *Electronic Notes in Theoretical Computer Science*, 2003.

[7] A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. Secure protocol composition (extended abstract). In *Proceedings of ACM Workshop on Formal Methods in Security Engineering*, pages 11–23, 2003.

[8] Anupam Datta, John C. Mitchell, and Dusko Pavlovic. Derivation of the JFK protocol. Technical report, Kestrel Institute, 2002.

[9] W. Diffie, P. C. Van Oorschot, and M. J. Wiener. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2:107–125, 1992.

[10] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[11] D. Dolev and A. Yao. On the security of public-key protocols. *IEEE Transactions on Information Theory*, 2(29), 1983.

[12] Nancy Durgin, John C. Mitchell, and Dusko Pavlovic. A compositional logic for protocol correctness. In *Proceedings of 14th IEEE Computer Security Foundations Workshop*, pages 241–255. IEEE, 2001.

[13] Warren D. Goldfarb. The undecidability of the second-order unification problem. *Theoretical Computer Science*, 13:225–230, 1981.

[14] Burton S. Kaliski, Jr. An unknown key-share attack on the mqv key agreement protocol. *ACM Transactions on Information and System Security (TISSEC)*, 4(3):275–288, 2001.

[15] Hugo Krawczyk. Sigma: The sign-and-mac approach to authenticated diffie-hellman and its use in the ike protocols. In *Advances in Cryptology - CRYPTO 2003*, volume 2729, pages 400–425. Springer-Verlag Heidelberg, 2003.

[16] Laurie Law, Alfred Menezes, Minghua Qu, Jerry Solinas, and Scott Vanstone. An efficient protocol for authenticated key agreement. Technical Report 98-05, COOR, 1998.

[17] G. Lowe. Some new attacks upon security protocols. In *Proceedings of 9th IEEE Computer Security Foundations Workshop*, pages 162–169. IEEE, 1996.

[18] Z. Manna and A. Pnueli. *Temporal Verification of Reactive Systems: Safety*. Springer-Verlag, 1995.

[19] T. Matsumoto, Y. Takashima, and H. Imai. On seeking smart public-key distribution systems. *The Transactions of the IECE of Japan*, E69:99–106, 1986.

[20] A. Menezes, M. Qu, and S. Vanstone. Some new key agreement protocols providing mutual implicit authentication. In *Workshop on Selected Areas in Cryptography (SAC '95)*, pages 22–32, 1995.

[21] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[22] Dusko Pavlovic and Douglas R. Smith. Composition and refinement of behavioral specifications. In *Automated Software Engineering 2001. The Sixteenth International Conference on Automated Software Engineering*. IEEE, 2001.

[23] Dusko Pavlovic and Douglas R. Smith. Guarded transitions in evolving specifications. In H. Kirchner and C. Ringeissen, editors, *Proceedings of AMAST 2002*, volume 2422 of *LNCS*, pages 411–425. Springer Verlag, 2002.

A A Protocol Logic

Protocol logic presented in [7]. Here, we only give a brief overview of the proof system.

A.1 Proof System

A.1.1 Axioms and Inference Rules

A representative fragment of the axioms and inference rules in the proof system are collected in Table 2. For expositional convenience, we divide the axioms into four groups.

The axioms about protocol actions state properties that hold in the state reached by executing one of the actions in a state in which formula ϕ holds. Note that the a in axiom **AA1** is any one of the 5 actions and a is the corresponding predicate in the logic.

VER and **SRC** respectively refer to the unforgeability of signatures and the need to possess the symmetric key in order to decrypt a message encrypted with that key. The additional condition requiring principal $\hat{X}$ to be honest guarantees that the intruder is not in possession of the private keys. These axioms (together with a few more axioms not described in this summary) provide an abstraction of the standard Dolev-Yao intruder model [11].

Axioms **P1**, **P2**, and **P3** capture the fact that most predicates are preserved by additional actions. For example, if in some state $\mathsf{Has}(X, n)$ holds, then it continues to hold, when X executes additional actions. Note, however, that the Fresh predicate is not preserved if the freshly generated value n is sent out in a message (see **F**).

The PLTL axioms **T1**, **T2**, and **T3** allow reasoning about the temporal ordering of actions. This turns out to be useful in proving authentication properties of protocols.

$\mathsf{Computes}$ shortcut and corresponding axioms (Table 3 allow us to reason about origination of some types of terms. Intuitively **CP2** says that there are two ways an agent can posses some term: he can construct it from components or he can receive it as a part of some message. Axiom **CP3** says that every term that appears on the network has a source — it originated from some process that actually computed the term.

They also capture hardness assumptions about cryptographic primitives. For example, we postulate that the only way to compute a Diffie-Hellman secret is to have one exponent and one exponential. Similarly, only way to compute a symmetric encryption is to have a key and the plaintext.

Axioms about Protocol Actions:

$$\begin{array}{ll} \mathbf{AA1} & \phi[a]_X \diamondminus (\mathsf{a} \wedge \ominus\phi) \\ \mathbf{AN3} & \phi[(\nu n)]_X \ \mathsf{Fresh}(X, n) \end{array}$$

Axioms Capturing Dolev-Yao Model:

$$\begin{array}{rl} \mathbf{VER} & \mathsf{Honest}(\hat{X}) \wedge \diamondminus \ \mathsf{Verify}(Y, \{\!|n|\!\}_{\overline{X}}) \supset \\ & \exists X.\exists m.(\diamondminus \mathsf{Send}(X, m) \wedge \mathsf{Contains}(m, \{\!|n|\!\}_{\overline{X}})) \\ \mathbf{SRC} & \mathsf{Source}(Z, t, E_K(t)) \wedge \mathsf{Has}(X, t) \wedge X \neq Z \supset \exists Y.\exists msg.(Y \neq B \wedge \mathsf{Has}(Y, K) \wedge \\ & \diamondminus \mathsf{Send}(Y, msg) \wedge \mathsf{Contains}(msg, t)) \end{array}$$

$$\begin{array}{rcl} \mathsf{Source}(Z, t, E_K(t)) & \equiv & (\mathsf{Computes}(X, t) \supset X = Z) \wedge ((\diamondminus \mathsf{Send}(Z, msg) \wedge \mathsf{Contains}(msg, t)) \supset \\ & & (m = \{t', E_K(t)\} \wedge \neg\mathsf{Contains}(t', t)) \end{array}$$

Preservation Axioms: (For $\mathsf{Persist} \in \{\mathsf{Has}, \diamondminus\phi\}$,)

$$\begin{array}{rl} \mathbf{P1} & \mathsf{Persist}(X, t)[a]_X \mathsf{Persist}(X, t) \\ \mathbf{P2} & \mathsf{Fresh}(X, t)[a]_X \mathsf{Fresh}(X, t), where(t \not\sqsubseteq a) \vee (a \neq \langle m \rangle) \\ \mathbf{P3} & \mathsf{HasAlone}(X, t)[a]_X \mathsf{HasAlone}(X, t), where(t \not\sqsubseteq_v a) \vee (a \neq \langle m \rangle) \\ \mathbf{F} & \mathsf{Fresh}(X, t)[\langle m \rangle]_X \neg\mathsf{Fresh}(X, t), where(t \sqsubseteq m) \end{array}$$

PLTL Axioms:

$$\begin{array}{ll} \mathbf{T1} & \diamondminus (\phi \wedge \psi) \supset (\diamondminus \phi \wedge \diamondminus \psi) \\ \mathbf{T2} & \diamondminus (\phi \vee \psi) \supset (\diamondminus \phi \vee \diamondminus \psi) \\ \mathbf{T3} & \ominus\neg\phi \leftrightarrow \neg\ominus\phi \end{array}$$

Temporal Ordering of actions:

$$\begin{array}{ll} \mathbf{AF1} & \theta[a_1 \ldots a_n]_X \ \mathsf{After}(\mathsf{a}_1, \mathsf{a}_2) \wedge \ldots \wedge \mathsf{After}(\mathsf{a}_{n-1}, \mathsf{a}_n) \\ \mathbf{AF2} & \mathsf{Honest}(\hat{X}) \wedge \mathsf{Honest}(\hat{Y}) \wedge \mathsf{Honest}(\hat{Z}) \supset \\ & (\mathsf{After}(\mathsf{a}_1(X), \mathsf{a}_2(Y)) \wedge \mathsf{After}(\mathsf{a}_2(\mathsf{Y}), \mathsf{a}_3(Z)) \supset \mathsf{After}(\mathsf{a}_1(X), \mathsf{a}_3(Z))) \\ \mathbf{AF3} & (\diamondminus (\mathsf{Send}(X, m) \wedge \ominus\mathsf{Fresh}(X, n)) \wedge \diamondminus \ \mathsf{a}(Y) \wedge \mathsf{Contains}(m, n) \wedge \mathsf{Contains}(a, n) \wedge (Y \neq X)) \\ & \supset \mathsf{After}(\mathsf{Send}(X, m), \mathsf{a}(Y)) \end{array}$$

Inference Rules:

$$\frac{\theta[P]_X\phi \quad \theta[P]_X\psi}{\theta[P]_X\phi \wedge \psi}\ \mathbf{G1} \qquad \frac{\theta[P]_X\phi \quad \theta' \supset \theta \quad \phi \supset \phi'}{\theta'[P]_X\phi'}\ \mathbf{G2} \qquad \frac{\phi}{\theta[P]_X\phi}\ \mathbf{G3} \qquad \frac{\phi}{\neg\diamondminus\neg\phi}\ \mathbf{TGEN}$$

Table 2: Fragment of the Proof System

$$
\begin{aligned}
\textbf{CP1} \quad & \mathsf{Computes}(X,t) \supset \mathsf{Has}(X,t) \\
\textbf{CP2} \quad & \mathsf{Has}(X,t) \supset \\
& (\mathsf{Computes}(X,t) \vee \exists m.(\diamondsuit\, \mathsf{Receive}(X,m) \wedge \mathsf{Contains}(m,t))) \\
\textbf{CP3} \quad & (\diamondsuit\, \mathsf{Receive}(X,m) \wedge \mathsf{Contains}(m,t)) \supset \\
& \exists Y.\exists m'.(\mathsf{Computes}(Y,t) \wedge \diamondsuit\, \mathsf{Send}(Y,m') \wedge \mathsf{Contains}(m',t)) \\
\mathsf{Computes}(X,t) \equiv\ & (t = g^{ab} \wedge \mathsf{Computes}_{\mathsf{DH}}(X, g^a b)) \vee \\
& (t = H(a) \wedge \mathsf{Computes}_{\mathsf{HASH}}(X, H(a))) \vee \\
& (t = E_a(b) \wedge \mathsf{Computes}_{\mathsf{ENC}}(X, E_a(b))) \\
\mathsf{Computes}_{\mathsf{DH}}(X, g^{ab}) \equiv\ & ((\mathsf{Has}(X,a) \wedge \mathsf{Has}(X, g^b)) \vee (\mathsf{Has}(X,b) \wedge \mathsf{Has}(X, g^a))) \\
\mathsf{Computes}_{\mathsf{ENC}}(X, E_a(b)) \equiv\ & \mathsf{Has}(X,a) \wedge \mathsf{Has}(X,b) \\
\mathsf{Computes}_{\mathsf{HASH}}(X, H(a)) \equiv\ & \mathsf{Has}(X,a)
\end{aligned}
$$

Table 3: Computes Axioms

A.1.2 The Honesty Rule

The honesty rule is essentially an invariance rule for proving properties of all roles of a protocol. It is similar to the basic invariance rule of LTL [18]. The honesty rule is used to combine facts about one role with inferred actions of other roles.

For example, suppose Alice receives a response from a message sent to Bob. Alice may wish to use properties of Bob's role to reason about how Bob generated his reply. In order to do so, Alice may assume that Bob is honest and derive consequences from this assumption. Since honesty, by definition in our framework, means "following one or more roles of the protocol," honest principals must satisfy every property that is a provable invariant of the protocol roles.

Since the honesty rule depends on the protocol, we write $\mathcal{Q} \vdash \theta[P]\phi$ if $\theta[P]\phi$ is provable using the honesty rule for $\mathcal{Q}$ and the other axioms and proof rules. Using the notation just introduced, the honesty rule may be written as follows.

$$
\frac{[\,]_X\ \phi \quad \forall \rho \in \mathcal{Q}.\forall P \epsilon BS(\rho).\ \phi\ [P]_X\ \phi}{\mathcal{Q} \vdash \mathsf{Honest}(\hat{X}) \supset \phi}\ \textbf{HON} \qquad \begin{array}{l}\text{no free variable} \\ \text{in } \phi \text{ except } X \\ \text{bound in } [P]_X\end{array}
$$

In words, if ϕ holds at the beginning of every role of $\mathcal{Q}$ and is preserved by all its basic sequences, then every honest principal executing protocol $\mathcal{Q}$ must satisfy ϕ. The side condition prevents free variables in the conclusion $\mathsf{Honest}(\hat{X}) \supset \phi$ from becoming bound in any hypothesis. Intuitively, since ϕ holds in the initial state and is preserved by all basic sequences, it holds at all pausing states of any run.

B Formal Protocol Correctness Proofs

A complete proof of the authentication property for the initiator role in CR template is given in Table 4.

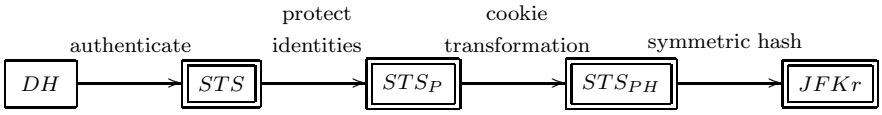

Figure 8: Derivation of the JFKr protocol

A complete proof of the secrecy property for the initiator role in ENC template is given in Table 5.

C Deriving the STS-MQV Family

C.1 Derivation of the JFKr Protocol

Our framework for deriving security protocols [5] seeks to systematize the practice of constructing protocols incrementally, starting from simple components and extending them by features and functions. In this section, we present, within this framework, a derivation of the $JFKr$ protocol. We use Diffie-Hellman key exchange and signature-based Challenge-Response as basic components. The derivation steps are shown in Figure C.1. As we proceed with the derivation, desired security properties accumulate. Among relevant properties are key secrecy, mutual authentication, denial-of-service protection and identity protection. This class of protocols is interesting partly because they form the basis of key exchange protocols for the IPSec protocol suite.

Diffie-Hellman component, DH

The basic Diffie-Hellman protocol [10] provides a way for two parties to set up a shared key (g^{xy}) which a passive attacker cannot recover.

$$A \to B : g^x$$
$$B \to A : g^y$$

There is no authentication guarantee for this protocol: the secret is shared between two parties, but neither can be sure of the identity of the other. The security of the key depends on the computational hardness of the discrete logarithm problem.

Using the derivation system, we want to transform this protocol into an authenticated key-exchange protocol. To achieve this goal, we first choose an authentication mechanism based on the exchange of fresh values. Then, we *compose* the two protocols, instantiating fresh values to Diffie-Hellman exponentials. The advantage of this modular approach is that an independent proof of security of the new protocol is not required. It can be deduced from the properties of the two components as long as they do not degrade each others security (for a detailed treatment of protocol composition ideas see [7]).

Challenge-Response protocol

The two-way challenge-response protocol based on signatures and encryption is shown below. Here, C_A and C_B represent certificates of A and B, while K_{AB} represents a secret key shared between A and B.

$$A \to B : m$$
$$B \to A : n, C_B, E_{K_{AB}}\left(SIG_B(n, m)\right)$$
$$A \to B : C_A, E_{K_{AB}}\left(SIG_A(m, n)\right)$$

$\mathbf{AA1}, \mathbf{T1}, \mathbf{P1}$	$[\mathbf{Init_{CR}}]_A \diamondsuit \mathsf{Receive}(A, msg) \wedge \mathsf{Contains}(msg, F(\hat{B}, \hat{A}, n, m))$	(1)
$\mathbf{CP3}, (1)$	$[\mathbf{Init_{CR}}]_A \exists X. \exists msg'. (\mathsf{Computes}(X, F(\hat{B}, \hat{A}, n, m)) \wedge$ $\diamondsuit \mathsf{Send}(X, msg') \wedge \mathsf{Contains}(msg', F(\hat{B}, \hat{A}, n, m)))$	(2)
Γ_{CR}	$\mathsf{Computes}(X, F(\hat{B}, \hat{A}, n, m)) \supset (\exists A'. X = A') \vee (\exists B'. X = B')$	(3)
$\mathbf{HON}$	$\mathsf{Honest}(\hat{Y}) \wedge \diamondsuit \mathsf{Send}(Y, msg') \supset \exists X. \exists x. \exists y. (\diamondsuit \mathsf{Fresh}(Y, y) \wedge$ $(msg' = \{\hat{Y}, \hat{X}, y\} \vee$ $msg' = \{\hat{Y}, \hat{X}, y, F(\hat{Y}, \hat{X}, y, x)\} \vee$ $msg' = \{\hat{Y}, \hat{X}, G(\hat{Y}, \hat{X}, y, x)\})$	(4)
Γ_{CR}	$\neg\mathsf{Contains}(\{\hat{A}, \hat{X}, m'\}, F(\hat{B}, \hat{A}, n, m))$	(5)
Γ_{CR}	$\mathsf{Contains}(\{\hat{A}, \hat{X}, G(\hat{A}, \hat{X}, m', x)\}, F(\hat{B}, \hat{A}, n, m)) \supset \hat{A} = \hat{B}$	(6)
Γ_{CR}	$\mathsf{Contains}(\{\hat{A}, \hat{X}, m', F(\hat{A}, \hat{X}, m', x)\}, F(\hat{B}, \hat{A}, n, m)) \supset \hat{A} = \hat{B}$	(7)
$(4-7)$	$\mathsf{Honest}(\hat{A}) \wedge \diamondsuit \mathsf{Send}(A', msg') \wedge \mathsf{Contains}(msg', F(\hat{B}, \hat{A}, n, m)) \supset$ $\hat{A} = \hat{B}$	(8)
$(2-3), (8)$	$[\mathbf{Init_{CR}}]_A \mathsf{Honest}(\hat{A}) \supset \exists B. \exists msg'. (\mathsf{Computes}(B, F(\hat{B}, \hat{A}, n, m)) \wedge$ $\diamondsuit \mathsf{Send}(B, msg') \wedge \mathsf{Contains}(msg', F(\hat{B}, \hat{A}, n, m)))$	(9)
Γ_{CR}	$\neg\mathsf{Contains}(\{\hat{B}, \hat{X}, n'\}, F(\hat{B}, \hat{A}, n, m))$	(10)
Γ_{CR}	$\mathsf{Contains}(\{\hat{B}, \hat{X}, G(\hat{B}, \hat{X}, n', x)\}, F(\hat{B}, \hat{A}, n, m)) \supset m = n'$	(11)
Γ_{CR}	$\mathsf{Contains}(\{\hat{B}, \hat{X}, n', F(\hat{B}, \hat{X}, n', x)\}, F(\hat{B}, \hat{A}, n, m)) \supset$ $\hat{A} = \hat{B} \wedge n = n' \wedge x = m$	(12)
$(4), (9-12)$	$[\mathbf{Init_{CR}}]_A \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(\hat{B}) \supset \exists B.$ $(\diamondsuit \mathsf{Send}(B, \{\hat{B}, \hat{X}, G(\hat{B}, \hat{X}, n', x)\}) \wedge \diamondsuit \mathsf{Fresh}(B, n') \wedge n' = m) \vee$ $(\diamondsuit \mathsf{Send}(B, \{\hat{B}, \hat{A}, n, F(\hat{B}, \hat{A}, n, m)\}))$	(13)
$\mathbf{AN3}, \mathbf{P1}$	$[\mathbf{Init_{CR}}]_A \diamondsuit \mathsf{Fresh}(A, m)$	(14)
$(13-14)$	$[\mathbf{Init_{CR}}]_A \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(\hat{B}) \supset$ $\diamondsuit \mathsf{Send}(B, \{\hat{B}, \hat{A}, n, F(\hat{B}, \hat{A}, n, m)\})$	(15)
$(15), \mathbf{HON}$	$[\mathbf{Init_{CR}}]_A \mathsf{Honest}(A) \wedge \mathsf{Honest}(\hat{B}) \supset \mathsf{ActionsInOrder}($ $\mathsf{Receive}(B, \{\hat{A}, \hat{B}, n\}), \mathsf{Send}(B, \{\hat{A}, \hat{B}, n, F(\hat{B}, \hat{A}, n, m)\}))$	(16)
$\mathbf{F}, \mathbf{AF3}$	$[\mathbf{Init_{CR}}]_A \mathsf{After}(\mathsf{Send}(A, \{\hat{A}, \hat{B}, n\}), \mathsf{Receive}(B, \{\hat{A}, \hat{B}, n\}))$	(17)
$\mathbf{F}, \mathbf{AF3}, \mathbf{HON}$	$[\mathbf{Init_{CR}}]_A \mathsf{Honest}(\hat{B}) \supset \mathsf{After}(\mathsf{Send}(B, \{\hat{A}, \hat{B}, n, F(\hat{B}, \hat{A}, n, m)\}),$ $\mathsf{Receive}(A, \{\hat{A}, \hat{B}, n, F(\hat{B}, \hat{A}, n, m)\}))$	(18)
$\mathbf{AF1}, \mathbf{AF2}$	$[\mathbf{Init_{CR}}]_A \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(\hat{B}) \supset \phi_{auth}$	(19)

Table 4: Deductions of $\hat{A}$ executing $\mathbf{Init_{CR}}$ role

$\mathbf{AA1}, \mathbf{T1}, \mathbf{P1}$	$[\mathbf{Init_{ENC}}]_A \diamondsuit \mathsf{Receive}(A, msg) \wedge$ $\mathsf{Contains}(msg, E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m)))$	(1)
$\mathbf{CP3}, (1)$	$[\mathbf{Init_{ENC}}]_A \exists X. \exists msg'.$ $(\mathsf{Computes}(X, E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m))) \wedge \diamondsuit \mathsf{Send}(X, msg') \wedge$ $\mathsf{Contains}(msg', E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m))))$	(2)
$\mathbf{HON}$	$[\mathbf{Init_{ENC}}]_A \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(\hat{B}) \wedge \mathsf{Has}(X, K_{AB}) \supset$ $(\exists A'. X = A') \vee (\exists B'. X = B')$	(3)
$\mathbf{HON}$	$\mathsf{Honest}(\hat{Y}) \wedge \diamondsuit \mathsf{Send}(Y, msg') \supset \exists X. \exists x. \exists y. (\diamondsuit \mathsf{Fresh}(Y, y) \wedge$ $(msg' = \{\hat{Y}, \hat{X}, y\} \vee$ $msg' = \{\hat{Y}, \hat{X}, y, E_{K_{XY}}(I(\hat{Y}, \hat{X}, y, x))\} \vee$ $msg' = \{\hat{Y}, \hat{X}, E_{K_{XY}}(H(\hat{Y}, \hat{X}, y, x))\})$	(4)
Γ_{ENC}	$\neg\mathsf{Contains}(\{\hat{A}, \hat{X}, m'\}, E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m)))$	(5)
Γ_{ENC}	$\mathsf{Contains}(\{\hat{A}, \hat{X}, E_{K_{AX}}(I(\hat{A}, \hat{X}, m', x))\},$ $E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m))) \supset \hat{A} = \hat{B}$	(6)
Γ_{ENC}	$\mathsf{Contains}(\{\hat{A}, \hat{X}, m', E_{K_{AX}}(H(\hat{A}, \hat{X}, m', x))\},$ $E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m))) \supset \hat{A} = \hat{B}$	(7)
$(2-7)$	$[\mathbf{Init_{ENC}}]_A \exists B. \exists msg'. (\diamondsuit \mathsf{Send}(X, msg') \wedge$ $\diamondsuit \mathsf{Fresh}(B, n) \wedge \mathsf{Contains}(msg', E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m))))$	(8)
Γ_{ENC}	$\neg\mathsf{Contains}(\{\hat{B}, \hat{X}, n'\}, H(\hat{B}, \hat{A}, n, m))$	(9)
Γ_{ENC}	$\neg\mathsf{Contains}(\{\hat{B}, \hat{X}, E_{K_{BX}}(I(\hat{B}, \hat{X}, n', x))\}, H(\hat{B}, \hat{A}, n, m))$	(10)
Γ_{ENC}	$\mathsf{Contains}(\{\hat{B}, \hat{X}, n', E_{K_{BX}}(H(\hat{B}, \hat{X}, n', x))\}, H(\hat{B}, \hat{A}, n, m)) \supset$ $n' = n \wedge m = x \wedge \hat{X} = \hat{A}$	(11)
Γ_{ENC}	$\mathsf{Computes}(X, H(\hat{B}, \hat{A}, n, m)) \supset \exists B. X = B$	(12)
$(4), (9-12)$	$[\mathbf{Init_{ENC}}]_A \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(\hat{(}B)) \supset$ $\mathsf{Source}(B, H(\hat{B}, \hat{A}, n, m), E_{K_{AB}}(H(\hat{B}, \hat{A}, n, m)))$	(13)
$(13), (5-7), \mathbf{SRC}$	$[\mathbf{Init_{ENC}}]_A \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(\hat{(}B)) \supset$ $\mathsf{Has}(X, H(\hat{B}, \hat{A}, n, m)) \supset \mathsf{Has}(X, K_{AB})$	(14)
$(14), (3)$	$[\mathbf{Init_{ENC}}]_A \mathsf{Honest}(\hat{A}) \wedge \mathsf{Honest}(\hat{(}B)) \supset \phi_{secrecy}$	(15)

Table 5: Deductions of $\hat{A}$ executing $\mathbf{Init_{ENC}}$ role

This protocol achieves mutual authentication, provided that m and n are fresh values.

There are many other mechanisms that we could have chosen here. For example, we could use only signatures, and have every participant include the peer's identity inside the signature.

By composing the above protocols, we obtain the following protocol. Fresh values m and n are instantiated to fresh Diffie-Hellman exponents g^x and g^y.

$$\begin{aligned} &A \to B : g^x \\ &B \to A : g^y, C_B, E_{K_{AB}}\left(SIG_B(g^y, g^x)\right) \\ &A \to B : C_A, E_{K_{AB}}\left(SIG_A(g^x, g^y)\right) \end{aligned}$$

This protocol retains the authentication property of the original challenge response protocol. Also, A and B end up with a shared secret after executing the protocol. Note however that an assumption here is that A and B already have a shared key K_{AB}. In the next step, we relax this assumption by instantiating K_{AB} to a key generated from the Diffie-Hellman secret g^{xy} during the execution of the protocol.

Protocol STS

By instantiating K_{AB} to a key K generated from a Diffie-Hellman shared secret g^{xy} we obtain the STS protocol.

$$\begin{aligned} &A \to B : g^x \\ &B \to A : g^y, C_B, E_K\left(SIG_B(g^y, g^x)\right) \\ &A \to B : C_A, E_K\left(SIG_A(g^x, g^y)\right) \end{aligned}$$

This protocol provides a way for two parties to set up a shared secret and guarantees a form of mutual authentication.

Protocol STS_P

In order to protect the identities of the participants against a passive attacker, we move the certificates inside the encryption. The resulting protocol is denoted by STS_P.

$$\begin{aligned} &A \to B : g^x \\ &B \to A : g^y, E_K\left(C_B, SIG_B(g^y, g^x)\right) \\ &A \to B : E_K\left(C_A, SIG_A(g^x, g^y)\right) \end{aligned}$$

In this protocol, the identities of both the participants are protected against passive attackers, while only the identity of the initiator A is protected against active attackers.

Protocol STS_{PH}

In order to make a protocol resistant to blind Denial-of-Service (DoS) attacks, we perform the *cookie transformation*. The responder B sends an unforgeable token to A and continues with the protocol only after receiving it back. In this case, the token used is just $HMAC_{BH}(g^y, g^x)$, where BH is B's private long term key used only for this purpose. The resulting protocol is denoted by STS_{PH}.

$$\begin{aligned} &A \to B : g^x \\ &B \to A : g^y, HMAC_{BH}(g^y, g^x) \\ &A \to B : g^x, g^y, HMAC_{BH}(g^y, g^x), E_K\left(C_A, SIG_A(g^x, g^y)\right) \\ &B \to A : E_K\left(C_B, SIG_B(g^y, g^x)\right) \end{aligned}$$

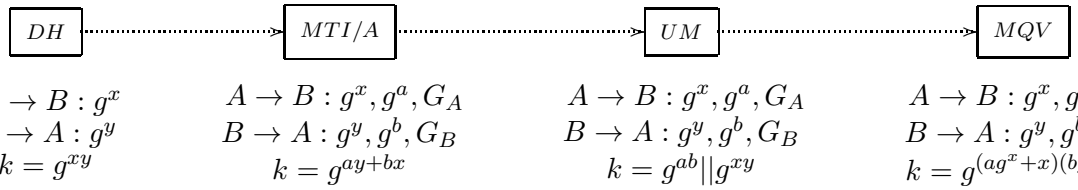

Figure 9: Refinements of the Diffie-Hellman key exchange

Under certain assumptions, the cookie transformation guarantees that the responder does not have to create state or perform expensive computation before a round-trip communication is established with the initiator. The cookie transformation is described in detail in [8]. Since we swapped the order of the last two messages, the initiator A reveals his identity first. Therefore, only the identity of the responder B is protected against active attackers.

Protocol $JFKr$

Encryptions are augmented with message authentication codes binding them to their source. Here K' is a key generated from the shared secret g^{xy} independently from K. This is the JFKr protocol minus nonces and reuse of Diffie-Hellman exponents, which can be added using one more refinement. Also, we omit some details from messages (e. g. security association and the group identifying information).

$$
\begin{aligned}
&A \to B : g^x \\
&B \to A : g^y, HMAC_{BH}(g^y, g^x) \\
&A \to B : g^x, g^y, HMAC_{BH}(g^y, g^x), E_K\left(C_A, SIG_A(g^x, g^y)\right), \\
&\qquad HMAC_{K'}\left(A, E_K\left(C_A, SIG_A(g^x, g^y)\right)\right) \\
&B \to A : E_K\left(C_B, SIG_B(g^y, g^x)\right), \\
&\qquad HMAC_{K'}\left(B, E_K\left(C_B, SIG_B(g^y, g^x)\right)\right)
\end{aligned}
$$

The final protocol inherits the security properties from the protocols in the earlier steps of the derivation: key secrecy, DoS protection and forms of mutual authentication and identity protection.

C.2 Refinements of Diffie-Hellman key exchange

In this section, we examine the structure of another family of protocols that has gone through the standardization process. Starting from the standard Diffie-Hellman protocol, we successively obtain protocols with more desirable security properties as the derivation proceeds. The derivation steps are shown in Figure C.2. The properties of interest include key secrecy, implicit authentication, forward secrecy, known-key security, resistance to unknown key share attacks, and efficiency.

Ephemeral Diffie-Hellman DH **key exchange**

The basic Diffie-Hellman protocol [10] provides a way for two parties to set up a shared key (g^{xy}) which a passive attacker cannot recover.

$$
\begin{aligned}
A &\to B : g^x \\
B &\to A : g^y
\end{aligned}
$$

$$k = g^{xy} = (g^y)^x = (g^x)^y$$

There is no authentication guarantee: the secret is shared between two parties, but neither can be sure of the identity of the other. One way to overcome this is for participants to have their public Diffie-Hellman values certified by a trusted authority (static Diffie-Hellman) and use those keys instead in the exchange. But, in that case, A and B would compute the same shared secret in every session, i.e, the protocol would not have known-key security.

MTI/A key exchange

The MTI/A protocol [19] tries to achieve authenticated key exchange by combining ephemeral and static Diffie-Hellman.

$$A \rightarrow B : g^x, g^a, G_A$$
$$B \rightarrow A : g^y, g^b, G_B$$

$$k = g^{ay+bx} = (g^y)^a (g^b)^x = (g^x)^b (g^a)^y$$

It is assumed that parties A and B have long term Diffie-Hellman exponents a and b and have obtained certificates G_A and G_B for corresponding public exponentials g^a and g^b. Also, x and y are generated fresh for every session and therefore, unique shared key is generated each time. It therefore provides known-key security, key secrecy, and implicit authentication. However, there is no forward secrecy since if the long-term secrets a and b are revealed, an attacker can compute all past session keys. Also, this protocol is open to an unknown key-share attack if an attacker can obtain certificates for exponentials of his choice without having to prove that he possesses the corresponding private exponents. The attack was first presented in [20].

UM key exchange

The *Unified model* protocol [3] represents another step forward. It combines ephemeral and static Diffie-Hellman in a very simple manner: the shared secret is just a concatenation of the ephemeral and static shared secrets.

$$A \rightarrow B : g^x, g^a, G_A$$
$$B \rightarrow A : g^y, g^b, G_B$$

$$k = g^{ab} || g^{xy}$$

Besides providing the security guarantees given by MTI/A (key secrecy, implicit authentication, and known-key security), it also provides perfect forward secrecy since the epheremal shared secrets cannot be computed even if the long term private keys are revealed and that is required to compute the session keys. However, this protocol is also open to an unknown key-share attack.

MQV key exchange

The final protocol in the derivation is MQV [16].

$$A \rightarrow B : g^x, g^a, G_A$$
$$B \rightarrow A : g^y, g^b, G_B$$

$$k = g^{(ag^x+x)(bg^y+y)} = (g^b)^{(ag^x+x)g^y} (g^y)^{ag^x+x} = (g^a)^{(bg^y+y)g^x} (g^x)^{bg^y+y}$$

It provides all but one of the desirable properties: key secrecy, implicit authentication, known-key security, forward secrecy, and computational efficiency. Note however that it is open to an unknown key-share attack as pointed out in [14].

C.3 Combining the patterns

In this section, we examine how security protocols can be constructed by combining design patterns. This approach enables exploration of the design space and helps identify tradeoffs between the various security properties. Specifically, the Diffie-Hellman component in the $JFKr$ derivation pattern is replaced by a more "refined" component from the second derivation pattern. This yields a class of protocols which inherit security properties from both the patterns. The derivation graph for the complete class is shown in Figure 5. Due to space constraints, we examine only one path in detail to get a sense of the general method.

C.3.1 Derivation of the JFK_r^{MQV} protocol

We start by composing the MQV component with the challenge-response protocol. Since the MQV shared secret includes certified static Diffie-Hellman exponentials, signatures are no longer necessary, resulting in protocols with less computational overhead.

Protocol STS^{MQV}

By composing the MQV key exchange with the challenge response protocol, we obtain the STS^{MQV} protocol. Fresh values m and n are instantiated to pairs of Diffie-Hellman exponents (g^x, g^a) and (g^y, g^b), and the key K is instantiated to a key generated from the MQV shared secret.

$$
\begin{aligned}
&A \rightarrow B : g^x, g^a \\
&B \rightarrow A : g^y, g^b, G_B, E_K\left(g^y, g^x\right) \\
&A \rightarrow B : G_A, E_K\left(g^x, g^y\right)
\end{aligned}
$$

This protocol inherits the key secrecy and mutual authentication properties from STS and forward secrecy, known-key security, and computational efficiency from MQV. Note that the unknown key-share attack on MQV goes away because STS provides explicit key authentication (not just implicit). This is an interesting illustration of the advantage of protocol construction through combining design patterns.

Protocol STS_P^{MQV}

In order to protect the identity of the participants against a passive attacker, we move the certificates inside the encryption. The resulting protocol is denoted by STS_P^{MQV}.

$$
\begin{aligned}
&A \rightarrow B : g^x, g^a \\
&B \rightarrow A : g^y, g^b, E_K\left(G_B, g^y, g^x\right) \\
&A \rightarrow B : E_K\left(G_A, g^x, g^y\right)
\end{aligned}
$$

While preserving the security properties achieved in the previous step, this protocol, in addition, provides a form of identity protection. The identities of both the participants are protected against passive attackers, while the identity of the initiator A is also protected against active attackers. Notice that the identity protection this protocol provides is much weaker than that of STS_P. Public keys are sent in the clear, and an attacker can deduce the identity of a participant if he possesses his certificate. This drawback is the result of using encryptions only, and not encrypted signatures. We cannot move public keys into the encryption since A needs to know g^b in order to generate the shared key K.

Protocol STS_{PH}^{MQV}

In order to make the protocol resistant to blind Denial-of-Service (DoS) attacks, we preform the *cookie transformation*. In this case, the token used is $HMAC_{BH}(g^y, g^x)$, where BH is B's private long term key used only for this purpose. The resulting protocol is denoted by STS_{PH}.

$$
\begin{aligned}
&A \to B : g^x, g^a \\
&B \to A : g^y, g^b, HMAC_{BH}(g^y, g^x) \\
&A \to B : g^x, g^a, g^y, g^b, HMAC_{BH}(g^y, g^x), E_K\left(G_A, g^x, g^y\right) \\
&B \to A : E_K\left(G_B, g^y, g^x\right)
\end{aligned}
$$

The other security properties are preserved under this transformation.

Protocol $JFKr^{MQV}$

Finally, we add message authentication codes to obtain $JFKr^{MQV}$ protocol.

$$
\begin{aligned}
&A \to B : g^x, g^a \\
&B \to A : g^y, g^b, HMAC_{BH}(g^y, g^x) \\
&A \to B : g^x, g^a, g^y, g^b, HMAC_{BH}(g^y, g^x), E_K\left(G_A, g^x, g^y\right) \\
&\qquad\quad HMAC_{K'}\left(A, E_K\left(G_A, g^x, g^y\right)\right), \\
&B \to A : E_K\left(G_B, g^y, g^x\right), \\
&\qquad\quad HMAC_{K'}\left(B, E_K\left(G_B, g^y, g^x\right)\right)
\end{aligned}
$$

The final protocol provides key secrecy, mutual authentication, forward secrecy, known-key security, computational efficiency, identity protection and DoS protection, inheriting most of the good qualities from the parent design patterns.