Maude-NPA, Version 2.0 (November 26th, 2011)

Santiago Escobar
sescobar@dsic.upv.es
DSIC-ELP, Universitat Politècnica de València
Valencia, Spain

Catherine Meadows
meadows@itd.nrl.navy.mil
Naval Research Laboratory
Washington, DC, USA

José Meseguer
meseguer@cs.uiuc.edu
University of Illinois at Urbana-Champaign
Urbana, IL, USA

Contents

1 Introduction

This document describes Version 2.0 of the Maude-NRL Protocol Analyzer (Maude-NPA) and gives instructions for its use. Maude-NPA is an analysis tool for cryptographic protocols that takes into account many of the algebraic properties of cryptosystems that are not included in other tools. These include cancellation of encryption and decryption, Abelian groups (including exclusive-or, exponentiation, and homomorphic encryption). Maude-NPA uses an approach similar to the original NRL Protocol Analyzer; it is based on unification, and performs backwards search from a final state to determine whether or not it is reachable. Unlike the original NPA, it has a theoretical basis in rewriting logic and narrowing, and offers support for a wider basis of equational theories that includes commutative (C), associative-commutative (AC), and associative-commutative-identity (ACU) theories. A description of Maude-NPA's formal foundations in rewriting logic, together with a soundness and completeness proof, are given in [12]. The most detailed description of how Maude-NPA works is given in [16]. Descriptions of how Maude-NPA handles different equational theories are given in [13, 10, 28, 11].

This document is organized as follows. In Section 2 we describe the mechanics of loading Maude-NPA and Maude-NPA specifications. In Section 3 we describe how a protocol is specified in Maude-NPA, using the Needham-Schroeder public key (NSPK) protocol as an example. We also describe how the algebraic properties of a protocol are specified and show the three possible ways: equational theories without extra properties, equational theories with commutative, associative-commutative or associative-commutative-identity symbols, and homomorphic encryption over concatenation. We illustrate these with cancellation of encryption and decryption, exclusive-or, modular exponentiation, and homomorphic encryption over concatenation. The reader can find in Appendix A the types of equational theories that Maude-NPA supports, and a description of how the user can ensure that the requirements are met in Section 3.2.6. In Section 4 we describe the commands that can be used, again using NSPK as an example. In Section 5 we describe how the tool can be applied to three other examples involving equational theories: (i) Needham-Schroeder-Lowe (NSL), where concatenation is replaced by exclusive or (exhibiting an attack not existing for the original NSL) (ii) NSL where encryption is homomorphic over concatenation (exhibiting an attack not existing for the original NSL), and (iii) the basic Diffie-Hellman protocol. In Section 7 we describe some known limitations of the tool and plans for further extensions. In several appendices we give some commands that are mainly used for debugging Maude-NPA, we describe how to specify grammars, which cut down many useless states, we give a brief description of other state-space reduction techniques supported by the tool, and we include the full specification of the protocol examples used in this document.

Throughout this document, we assume a minimum acquaintance with the basic syntactic conventions of the Maude language, an implementation of rewriting logic. We refer the user to the Maude manual that is available online at `maude.cs.uiuc.edu`, and also to the Maude book [5] for more detailed documentation on Maude-related matters.

2 Setting Up and Using Maude-NPA

We assume that the user has installed a copy of Maude that includes the implementation of order-sorted C, AC, and ACU unification, e.g., version 2.6 or later. After starting Maude, the user must load Maude-NPA. To do this, the user must be in the Maude-NPA directory. The user should type the command

```
load maude-npa
```

All Maude-NPA specification files must end with the suffix `.maude`, e.g., `foo.maude`. Instructions for writing specifications are given in Section 3. In order to load a specification one uses the `cd` command to change to the directory that the specification is in, and then types the command

```
load foo
```

If the user does not want to change to the directory where `foo.maude` sits in, it is necessary to specify the directory path when loading it, e.g., `load examples/foo`.

Once `foo.maude` is loaded, it is possible to search for attacks using the commands described in Section 4.

3 Protocol Specifications

Protocol specifications are given in a single file (e.g., `foo.maude`), and consist of three Maude modules, having a fixed format and fixed module names. In the first module, the *syntax* of the protocol is specified, consisting of sorts and operators. The second module specifies the *algebraic properties* of the operators. Note that algebraic properties must satisfy some specific conditions given in Section 3.2 and Appendix A. The third module specifies the *actual behavior of the protocol* using a strand-theoretic notation. This module includes the intruder strands (also called Dolev-Yao strands) and regular strands (describing the behavior of principals). It also contains *attack states* describing behavior that we want to prove cannot occur.

We give a template for any Maude-NPA specification below. Throughout, lines beginning with three or more dashes (i.e., `---`) or three or more asterisks (i.e., `***`) are comments that are ignored by Maude.

```
fmod PROTOCOL-EXAMPLE-SYMBOLS is
  --- Importing sorts Msg, Fresh, and Public
  protecting DEFINITION-PROTOCOL-RULES .
  ----------------------------------------------------------
  --- Overwrite this module with the syntax of your protocol
  --- Notes:
  --- * Sorts Msg and Fresh are special and imported
  --- * Sorts must be subsorts of Msg
  --- * No sort can be a supersort of Msg
  --- * Variables of sort Fresh are really fresh
  ---   and no substitution is allowed on them
  --- * Sorts Msg and Public cannot be empty
  ----------------------------------------------------------
endfm

fmod PROTOCOL-EXAMPLE-ALGEBRAIC is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .
  ----------------------------------------------------------------
  --- Overwrite this module with the algebraic properties
  --- of your protocol
  --- * Use only equations of the form (eq Lhs = Rhs [nonexec] .)
  --- * Attribute owise cannot be used
  --- * There is no order of application between equations
  ----------------------------------------------------------------

endfm

fmod PROTOCOL-SPECIFICATION is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .
  protecting DEFINITION-PROTOCOL-RULES .
  protecting DEFINITION-CONSTRAINTS-INPUT .

  ----------------------------------------------------------
  --- Overwrite this module with the strands
  --- of your protocol and the attack states
  ----------------------------------------------------------

  eq STRANDS-DOLEVYAO
   = --- Add Dolev-Yao strands here. Strands are properly renamed
  [nonexec] .

  eq STRANDS-PROTOCOL
   = --- Add protocol strands here. Strands are properly renamed
  [nonexec] .

  eq ATTACK-STATE(0)
   = --- Add attack state here
     --- More than one attack state can be specified, but each must be
     ---    identified by a number (e.g. ATTACK-STATE(1) = ...
     ---     ATTACK-STATE(2) = ... etc.)
  [nonexec] .

endfm

--- THIS HAS TO BE THE LAST ACTION !!!!
select MAUDE-NPA .
```

In what follows we explain in detail how each of these three modules describing a Maude-NPA specification are specified.

3.1 Specifying the Protocol Syntax

The protocol syntax is specified in the module `PROTOCOL-EXAMPLE-SYMBOLS`. Note that, since we are using Maude also as the specification language, each declaration has to be ended by a space and a period.

3.1.1 Sorts and Subsorts

We begin by specifying *sorts*. In general, sorts are used to specify different types of data, that are used for different purposes. We have a special sort called `Msg` that represents what a message is going to look like in our protocol. If a protocol makes no additional sort distinctions, i.e., if it is an unsorted protocol, there will be no extra sorts, and every symbol will be of sort `Msg`. However, if only keys can be used for encryption, we would like to have a sort `Key`, and specify that an encryption operator `e` can only take a term of sort `Key` as its first argument, e.g., "`op e : Key Msg -> Msg`."

Sorts can also be *subsorts* of other sorts. Subsorts allow a more refined distinction of data within a concrete sort. For example we might have a sort `Masterkey` which is a subsort of `Key`. Or two sorts `PublicKey` and `PrivateKey`, which are subsorts of `Key`. These two relevant subsort relations can be specified in Maude as follows:

```
subsort MasterKey < Key .
subsorts PublicKey PrivateKey < Key .
```

Most sorts are user-defined. However, there are several special sorts that are automatically imported by any Maude-NPA protocol definition, and for which the user must make sure that certain constraints are satisfied. These are:

`Msg` Sorts defined by the user must be subsorts of `Msg`. No sort defined by the user can be a supersort of `Msg`. This sort cannot be empty, i.e., it is necessary to define at least one symbol of sort `Msg` or of a subsort of `Msg`.

`Fresh` The sort `Fresh` is used to identify terms that must be unique. It is typically used as an argument of some data that must be unique, such as a nonce, or a session key, e.g., "`n(A,r)`" or "`k(A,B,r)`" where `r` is a variable of sort `Fresh`. It is not necessary to define symbols of sort `Fresh`, i.e., the sort `Fresh` can be empty.

`Public` The sort `Public` is used to identify terms that are publically available, and therefore assumed known by the intruder[1]. This sort cannot be empty.

[1] The `Public` sort will be automatically deduced in future versions of the tool.

We begin with the definition of sorts. We use the Needham-Schroeder Public Key Protocol (NSPK) as a running example. This protocol uses public key cryptography, and the principals exchange encrypted data consisting of names and nonces. Thus we will define sorts to distinguish names, keys, nonces, and encrypted data. This is specified as follows:

```
--- Sort Information
sorts Name Nonce .
subsort Name Nonce < Msg .
subsort Name < Public .
```

The sorts `Nonce` and `Name` are not strictly necessary, but they can make the search more efficient. Maude-NPA will not attempt to unify terms with incompatible sorts. So, for example, in this specification, if a principal is expecting a term of sort `Name`, then will not accept a term of sort `Nonce`; technically because `Name` is not declared as a subsort of `Nonce`. If we are looking for type confusion attacks, we would not want to include these sorts, and would instead declare everything as having sort `Msg`. See [13] for an example of a type confusion attack.

We can now specify the different operators needed in NSPK. These are `pk` and `sk`, for public and private key encryption, the operator `n` for nonces, designated constants for principals, and concatenation using the infix operator "`;`".

We begin with the public/private encryption operators.

```
--- Encoding operators for public/private encryption
op pk : Name Msg -> Msg [frozen] .
op sk : Name Msg -> Msg [frozen] .
```

The `frozen` attribute is technically necessary to tell Maude not to attempt to apply rewrites at arguments of those symbols[2]. The `frozen` attribute must be included in all operator declarations in Maude-NPA specifications, excluding constants. The use of sort `Name` as an argument of public key encryption may seem odd at first. But it is used because we are implicitly associating a public key with a name when we apply the `pk` operator, and a private key with a name when we apply the `sk` operator. A different syntax specifying explicit keys could have been chosen for public/private encryption.

Next we specify some principal names. These are not all the possible principal names. Since Maude-NPA is an unbounded session tool, the number of possible principals is unbounded. This is achieved by using variables (i.e., of sort `Name` in NSPK) instead of constants. However, we may have a need to specify constant principal names in a goal state. For example, if we have an initiator and a responder, and we are not interested in the case in which the initiator and the responder are the same, we can prevent that by specifying the names of the initiator and the responder as different constants. Also, we may want to identify the intruder's name

[2] The `frozen` attribute will be automatically introduced in future versions of the tool.

by a constant, so that we can cover the case in which principals are talking directly to the intruder.

For NSPK, we have three constants of sort Name: a, b, and i.

```
--- Principals
op a : -> Name . --- Alice
op b : -> Name . --- Bob
op i : -> Name . --- Intruder
```

We now need two more operators, one for nonces, and one for concatenation. The nonce operator is specified as follows.

```
--- Nonce operator
op n : Name Fresh -> Nonce [frozen] .
```

Note that the nonce operator has an argument of sort Fresh to ensure uniqueness. The argument of type Name is not strictly necessary, but it provides a convenient way of identifying which nonces are generated by which principals. This makes searches more efficient, since it allows us to keep track of the originator of a nonce throughout a search. We could make things even more specific by keeping track of whether the originator was playing the role of initiator or responder, and including that as another argument. This would require us to define a new sort and use it as follows:

```
op init : -> Role .
op resp : -> Role .

op n : Name Role Fresh -> Nonce [frozen] .
```

Finally, we come to the concatenation operator. In Maude-NPA, we specify concatenation via an infix operator ";" defined as follows:

```
--- Concatenation operator
op _;_ : Msg Msg -> Msg [gather (e E) frozen] .
```

The Maude operator attribute "gather (e E)" indicates that symbol ";" has to be parsed as associated to the left; whereas "gather (E e)" indicates association to the right. Note that this is just a parsing attribute, and therefore different from the associativity equational property described in Section 3.2.2.

3.2 Algebraic Properties

The Maude-NPA performs symbolic reachability analysis *modulo* the equational theory of the protocol. This makes Maude-NPA verification much stronger than verification methods based on a purely syntactic view of the algebra of messages as a term algebra using the standard Dolev-Yao model of perfect cryptography in which no algebraic properties are assumed. Indeed, it is well-known (see, e.g., [29]) that various protocols that have been proved secure under the standard Dolev-Yao model can be broken by an attacker who exploits the algebraic properties of some cryptographic functions. For example, the Needham-Schroeder public key (NSPK) protocol has a man-in-the-middle-attack found by the Maude-NPA (see Section 4), whereas the Needham-Schroeder-Lowe (NSL) protocol is proved to be secure by the Maude-NPA (see Section 4.1). However, by adding equational properties to some symbols in the NSL protocol, namely replacing concatenation by exclusive-or or making encryption homomorphic over concatenation, Maude-NPA is able to find two new attacks (see Sections 5.1 and 5.2).

There are three types of algebraic properties: (i) *equational axioms*, such as commutativity (C), associativity-commutativity (AC), and associativity-commutativity-identity (ACU) called *axioms* in this manual, (ii) *equational rules*, called *variant equations* in this manual, and (iii) equational rules for dedicated unification algorithms, called *dedicated equations* in this manual. Variant and dedicated equations are specified in the `PROTOCOL-EXAMPLE-ALGEBRAIC` module, whereas axioms are specified within the operator declarations in the `PROTOCOL-EXAMPLE-SYMBOLS` module, as illustrated in what follows. Note that combinations of all three different types of algebraic properties will be available in the future but in the current version only axioms and variant equations can be combined.

3.2.1 The PROTOCOL-EXAMPLE-ALGEBRAIC Module

An equation is oriented into a rewrite rule in which each substitution instance of the left–hand side of the equation is *reduced* to the corresponding substitution instance of the right–hand side. In writing equations, one needs to specify the variables involved, and their type. Variables can be specified globally for a module, e.g., `var Z : Msg .`, or locally within the expression using it, e.g., a variable `A` of sort `Name` in “`pk(A:Name,Z)`”. Several variables of the same sort can be specified together, as “`vars X Y Z1 Z2 :  Msg .`”. In NSPK, we use two equations specifying the relationship between public and private key encryption, as follows:

```
eq pk(A:Name,sk(A:Name,Z:Msg)) = Z:Msg [nonexec metadata "variant"] .
eq sk(A:Name,pk(A:Name,Z:Msg)) = Z:Msg [nonexec metadata "variant"] .
```

The attribute `metadata "variant"` specified that these equations are not regular Maude equations, typically used for simplification, but equations for the variant-based unification algorithm available in Maude (see Appendix A.3 and [19, 9] for details on this unification algorithm). The `nonexec` attribute is technically necessary to tell Maude not to use an equation or rule within its standard execution, since it will be used only in the narrowing implementation[3] for unification purposes. The `nonexec` attribute must be included in all user-defined equation and rule declarations of the protocol. Furthermore, the attribute `owise` (i.e., otherwise) for equations in Maude cannot be used and no order of application is assumed on the algebraic properties.

[3] The `nonexec` attribute will be automatically introduced in future versions of the tool.

3.2.2 Specifying Theories with C, AC, or ACU Symbols

Since Maude-NPA uses special unification algorithms for the case of having commutative (C), associative-commutative (AC), or associative-commutative-identity (ACU) algebraic properties, these are specified not as standard equations but as *axioms* in the operator declarations. For example, suppose that we want to specify an exclusive-or operator but without self cancellation. If we add no other algebraic property, then we specify an infix associative-commutative operator "*" with identity element null in the PROTOCOL-EXAMPLE-SYMBOLS module as follows:

```
op null : -> Msg .
op _*_ : Msg Msg -> Msg [frozen assoc comm id: null] .
```

where the associativity, commutativity, and identity axioms are declared as attributes of the * operator with the assoc, comm, and id: keywords. If we do not desire the identity property, i.e., only the associative-commutative operator "*", we would declare the * operator with the assoc and comm keywords. Similarly, we would specify an operator that is commutative but not associative with the comm keyword alone. [4]

3.2.3 Combining Variant Equations with Axioms: Exclusive or

Suppose that we want to specify the full theory of exclusive-or with self cancellation. We specify an infix associative-commutative operator "*" in the PROTOCOL-EXAMPLE-SYMBOLS module as follows:

```
op _*_ : Msg Msg -> Msg [frozen assoc comm] .
op null : -> Msg .
```

where the associativity and commutativity axioms are declared as in Section 3.2.2. We specify the cancellation rules for * in the PROTOCOL-EXAMPLE-ALGEBRAIC module as follows:

```
eq X:Msg * X:Msg * Y:Msg = Y:Msg [nonexec metadata "variant"] .
eq X:Msg * X:Msg = null [nonexec metadata "variant"] .
eq X:Msg * null = X:Msg [nonexec metadata "variant"] .
```

Note that the first equational property, i.e., X * X * Y = Y, is not part of the exclusive-or theory but it is necessary for coherence, see Section 3.2.6. Note also that, for termination reasons, exclusive-or should not be declared as an ACU symbol in Maude-NPA but only as an AC symbol with an explicit variant equation for the identity property (see Section 3.2.6 for technical details).

[4] It is also possible to specify and operator that is associative but not commutative using the assoc keyword, but this is not advised, since associative unification is not finitary. A form of *bounded* associativity is possible, but this is done differently, see [13] for details.

3.2.4 Combining Variant Equations with Axioms: Diffie-Hellman

If we want to include a Diffie-Hellman mechanism, we need two operations. One is exponentiation, and the other is modular multiplication. Since Diffie-Hellman is a commonly used algorithm in cryptographic protocols, we discuss key aspects of this theory in detail.

We begin by including several new sorts in PROTOCOL-EXAMPLE-SYMBOLS: Gen, Exp, GenvExp, and NeNonceSet.

```
sorts Name Nonce NeNonceSet Gen Exp Key GenvExp Secret .
subsort Gen Exp < GenvExp .
subsort Name NeNonceSet GenvExp Secret Key < Msg .
subsort Exp < Key .
subsort Nonce < NeNonceSet .
subsort Name < Public .
subsort Gen < Public .
```

We now introduce *three* new operators. The first, g, is a constant that serves as the Diffie-Hellman generator. The second is exponentiation, and the third is an associative-commutative multiplication operation on nonces.

```
op g : -> Gen .
op exp : GenvExp NeNonceSet -> Exp [frozen] .
op _*_ : NeNonceSet NeNonceSet -> NeNonceSet [frozen assoc comm] .
```

We then include the following equational property, to capture the fact that $z^{x^y} = z^{x*y}$:

```
eq exp(exp(W:Gen,Y:NeNonceSet),Z:NeNonceSet)
 = exp(W:Gen, Y:NeNonceSet * Z:NeNonceSet) [nonexec metadata "variant"] .
```

There are several things to note about this Diffie-Hellman specification. The first is that, although modular multiplication has a unit and inverses, this is not included in our equational specification. Instead, we have only included the algebraic property that is necessary for Diffie-Hellman to work. The second is that we have specified types that will rule out certain kinds of intruder behavior. In actual fact, there is nothing that prevents an intruder from sending an arbitrary string to a principal and passing it off as an exponentiated term. The principal will then exponentiate that term. However, given our definition of the exp operator, only terms of type GenvExp can be exponentiated. This last restriction is necessary in order to assure that the unification algorithm is finitary. The details of this are explained in Section 3.2.6 and Appendix A.3. The omission of units and inverses is not necessary to ensure finitary unification, but rules out behavior of the intruder that is likely to be irrelevant for attacking the protocol, or that is likely to be easily detected (such as the intruder sending an exp(g,0)).

We note that, if one is interested in obtaining a proof of security using these restrictive assumptions, one must provide a proof (outside of the tool) that security in the restricted model implies security in the more general model. This could be done along the lines of the proofs in [27, 24, 25].

3.2.5 Specifying Theories with Homomorphic Operators

Maude-NPA relies on three different kinds of algebraic properties:

- When *axioms* are the only algebraic properties, as it is the case of symbols having only commutative (C), associative-commutative (AC), or associative-commutative-identity (ACU) algebraic properties (this case was demonstrated in Section 3.2.2).
- When *variant equations* (with or without axioms) describe the algebraic properties (this case was demonstrated in Sections 3.2.3 and 3.2.4).
- When the algebraic properties do not fit into the two previous cases, *dedicated unification algorithms* for special equational theories can be designed and implemented into Maude-NPA. In this case, some *dedicated equations* are associated to the special equational theory in order for Maude-NPA to identify when such an special equational theory is being used by a protocol specification and to invoke the dedicated unification algorithm in the appropriate way.

We have initiated the development of dedicated specific unification algorithms for two purposes: (i) allow unification for equational theories not supported by the combination of axioms and variant equations (e.g. homomorphic operators, see Section 3.2.7) and (ii) to improve efficiency for commonly used theories (e.g. exclusive or or Abelian groups).

Currently, we have integrated one dedicated unification algorithm for encryption being homomorphic over concatenation, i.e., satisfying the following generic algebraic property

$$e(X;Y,Key) = e(X,Key);e(Y,Key)$$

However, the actual chosen symbols e and `_;_` are user definable. For example, suppose that we want to specify a version of the Needham-Schroeder-Lowe (NSL) protocol, which is a version of the Needham-Schroeder public key (NSPK) protocol fixed by Lowe to avoid flaws, but including the algebraic property that encryption is homomorphic over concatenation. Then, the dedicated equation added to the `PROTOCOL-EXAMPLE-ALGEBRAIC` module is as follows:

```
eq pk(X:Msg ; Y:Msg, K:Key) = pk(X:Msg, K:Key) ; pk(Y:Msg, K:Key)
     [nonexec label homomorphism metadata "builtin-unify"] .
```

Similarly to the inclusion of variant equations, this dedicated equation contains the `nonexec` attribute and a metadata attribute. However, two new syntactic features are added in order for the Maude-NPA to identify the appropriate dedicated equation:

1. A label "homomorphism" is explicitly used to identify this equation. This would help in the future when different dedicated algorithms may be combined.

2. A generic metadata “builtin-unify” is used to separate dedicated equations from variant equations. This would help in the future when variant and dedicated equations may be combined.

Note that this equational property forces the key to be the second argument of the encryption. Also, only one encryption symbol can be homomorphic over concatenation, that is, only one dedicated equation with the label “homomorphism” is allowed. Furthermore, at present all other symbols in the protocol cannot have commutative (C), associative-commutative (AC), or associative-commutative-identity (ACU) algebraic properties.

3.2.6 General Requirements for Variant Algebraic Theories

As explained in Appendix A, for theories which can be decomposed into a set of axioms and a set of equations and satisfy the requirements explained in this section, Maude-NPA uses a technique called *narrowing* to perform unification of symbolic terms *modulo* the variant equations specified for the algebraic properties of the protocol. In order for this narrowing technique to provide a *finite* set of unifiers, seven specific requirements must be met by any algebraic theory specifying cryptographic functions that the user provides. If these requirements are not satisfied, Maude-NPA may exhibit non-terminating and/or incomplete behavior, and any completeness claims about the results of the analysis cannot be guaranteed. We list below these seven requirements, explain in detail what they mean, and show in Section 3.2.7 how they are all met by the examples presented in Section 3.2.1.

Mathematically, an algebraic theory T is a pair of the form $T = (\Sigma, E \cup Ax)$, where Σ is a *signature* declaring sorts, subsorts, and function symbols (in Maude Σ is defined by the sort and subsort declarations and the operator declarations, as we have already illustrated with examples), and where $E \cup Ax$ is a set of *equations*, that we assume is split into a set Ax of equational axioms such as our previous combinations of associativity and/or commutativity and identity axioms, and a set E of oriented equations to be used from left to right as rewrite rules. In Maude, the axioms Ax are declared together with their corresponding operator declarations by means of the `assoc` and/or `comm` and/or `id:` attributes; they are *not* declared as explicit equations. Instead, the equations E are declared with the `eq` keyword as we have illustrated with examples.

In the Maude-NPA we call an algebraic theory $T = (\Sigma, E \cup Ax)$ specified by the user for the cryptographic functions of the protocol *admissible* if it satisfies the following seven requirements:

1. The axioms Ax can declare some binary operators in Σ to be commutative (with the `comm` attribute), associative-commutative (with the `assoc` and `comm` attributes) or associative-commutative-identity (with the `assoc`, `comm`, and `id:` attributes). No other combinations of axioms are allowed; that is, a function symbol has either no attributes, or only the `comm` attribute, or only the `assoc` and `comm` attributes, or only the `assoc`, `comm`, and `id:` attributes.

2. The equations E are confluent modulo Ax.

3. The equations E are terminating modulo Ax.

4. The equations E are coherent modulo Ax (see [23]).

5. The equations E are sort-decreasing.

6. The equations E are strongly right irreducible (see [19]).

7. The equations E are variant-preserving (see [19]).

We now explain in detail what these requirements mean.

Rewriting modulo Axioms Since Ax-unification is supported for the combinations of axioms Ax described in requirement (1), this implies that *Ax-matching* (the special case in which one of the terms being unified is a ground term without any variables) is supported, so that we in effect can use the equations E to rewrite terms *modulo Ax*. This is of course supported by Maude for axioms such as associativity, commutativity, and identity. Suppose, for example, that a + symbol has been declared commutative with the `comm` attribute, and that we have an equation in E of the form $x + 0 = x$. Then we can apply such an equation to the term $0 + 7$ *modulo* commutativity, even though the constant 0 is on the left of the + symbol. That is, the term $0 + 7$ *matches* the left-hand side pattern $x + 0$ *modulo* commutativity. We would express this rewrite step of simplification modulo commutativity with the arrow notation:

$$0 + 7 \to_{E/Ax} 7$$

where E is the set of equations containing the above equation $x + 0 = x$, and where Ax is the set of axioms containing the commutativity of $+$. Likewise, we denote by $\longrightarrow^*_{E/Ax}$ the reflexive-transitive closure of the one-step rewrite relation $\longrightarrow_{E/Ax}$ with the equations E modulo the axioms Ax. That is, $\longrightarrow^*_{E/Ax}$ corresponds to taking zero, one, or more rewrite steps with the equations E modulo Ax.

Confluence The equations E are called *confluent* modulo Ax if and only if for each term t in the theory $T = (\Sigma, E \cup Ax)$, if we can rewrite t with E modulo Ax in two different ways as: $t \longrightarrow^*_{E/Ax} u$ and $t \longrightarrow^*_{E/Ax} v$, then we can always further rewrite u and v to a common term modulo Ax. That is, we can always find terms u', v' such that:

- $u \longrightarrow^*_{E/Ax} u'$ and $v \longrightarrow^*_{E/Ax} v'$, and
- $u' =_{Ax} v'$

That is, u' and v' are essentially the same term, in the sense that they are equal modulo the axioms Ax. In our above example we have, for instance, $0+7 =_{Ax} 7+0$.

Termination The equations E are called *terminating* modulo Ax if and only if all rewrite sequences terminate; that is, if and only if we never have an infinite sequence of rewrites

$$t_0 \rightarrow_{E/Ax} t_1 \rightarrow_{E/Ax} t_2 \ldots t_n \rightarrow_{E/Ax} t_{n+1} \cdots$$

Coherence Rather than explaining the *coherence modulo Ax* notion in general (the precise definition of the general notion can found in [23]), we explain in detail its meaning in the case where it is needed for the Maude-NPA, namely, the case of AC and ACU symbols. The best way to illustrate the meaning of coherence is by its *absence*. Consider, for example, an exclusive or operator $\oplus$ which has been declared AC. Now consider the equation $x \oplus x = 0$. This equation, if not completed by another equation, is *not* coherent modulo AC. What this means is that there will be term *contexts* in which the equation *should* be applied, but it cannot be applied. Consider, for example, the term $b \oplus (a \oplus b)$. Intuitively, we should be able to apply the above equation to simplify it to the term $a \oplus 0$ in one step. However, we cannot! The problem is that the equation cannot be applied (even if we match modulo AC) to either the top term $b \oplus (a \oplus b)$ or the subterm $a \oplus b$. We can however make our equation coherent modulo AC by adding the extra equation $x \oplus x \oplus y = 0 \oplus y$, which using also the equation $x \oplus 0 = x$ we can slightly simplify to the equation $x \oplus x \oplus y = y$. This second variant of our equation will now apply to the term $b \oplus (a \oplus b)$, giving the simplification $b \oplus (a \oplus b) \longrightarrow_{E/Ax} a$.

For the Maude-NPA, coherence is only an issue for AC and ACU symbols. And there is always an easy way, given a set E of equations, to make them coherent. The method is as follows. For any symbol f which is AC, and for any equation of the form $f(u, v) = w$ in E, we add also the equation $f(f(u, v), x) = f(w, x)$, where x is a fresh new variable. In an order-sorted setting, we should give to x *the biggest sort possible*, so that it will apply in all generality. As an additional optimization, note that some equations may already be coherent modulo AC or ACU, so that we need not add the extra equation. For example, if the variable x has the biggest possible sort it could have, then the equation $x \oplus 0 = x$ is already coherent, since x will match "the rest of the $\oplus$-expression," regardless of how big or complex that expression might be, and of where in the expression a constant 0 occurs. For example, this equation will apply modulo AC to the term $(a \oplus (b \oplus (0 \oplus c))) \oplus (c \oplus a)$, with x matching the term $(a \oplus (b \oplus c)) \oplus (c \oplus a)$, so that we indeed get a rewrite $(a \oplus (b \oplus (0 \oplus c))) \oplus (c \oplus a) \rightarrow_{E/Ax} (a \oplus (b \oplus c)) \oplus (c \oplus a)$. Also, if we assume that symbol $\oplus$ is ACU instead of AC, then the previous three equations $x \oplus 0 = x$, $x \oplus x = 0$ and $x \oplus x \oplus y = y$ for $*$ being AC can be simplified into one equation $x \oplus x \oplus y = y$ for $*$ being ACU with 0 as the identity symbol. Note that this equation is coherent modulo ACU but it is not terminating modulo ACU since for any term T, we have $T =_{ACU} 0 \oplus 0 \oplus T$ and $0 \oplus 0 \oplus T \rightarrow_{E/ACU} T$ using the equation $x \oplus x \oplus y = y$ (i.e., exclusive or must be specified in Maude-NPA with an AC symbol and never with an ACU symbol).

Sort-decreasingness Sort-decreasingness is simple to explain with an example. If for the cancellation of encryption and decryption, we assume one subsort Encoding of the sort Msg and the following definitions for symbols pk and sk:

```
  --- Encoding operators for public/private encryption
 op pk : Name Msg -> Encoding [frozen] .
 op sk : Name Msg -> Encoding [frozen] .
```

Then the following equations for cancellation are not sort-decreasing, since the left-hand sides are defined as elements of sort Encoding but the application of the equations may return elements of a greater sort Msg:

```
eq pk(A:Name,sk(A:Name,Z:Msg)) = Z:Msg [nonexec metadata "variant"] .
eq sk(A:Name,pk(A:Name,Z:Msg)) = Z:Msg [nonexec metadata "variant"] .
```

Strongly Right Irreducible Given a theory $T = (\Sigma, E \cup Ax)$, which we assume satisfies conditions (1)–(5) above, we call the set E of equations *strongly right irreducible* iff for each equation $t = t'$ in E, we cannot further simplify by the equations E modulo Ax either the term t', or any substitution instance $\theta(t')$ where the terms in the substitution θ cannot themselves be further simplified by the equations E modulo Ax. Obvious cases of such righthand-sides t' include:

- a single variable;
- a constant for which no equations exist;
- a *constructor term*, that is, a term whose function symbols have no associated equations.

But these are not the only possible cases where strong right irreducibility can be applied. Typing, particularly the use of sorts and subsorts in an order-sorted equational specification, can greatly help in obtaining right irreducibility. We refer the reader to [13, 10] for two examples of how order-sorted typing helps narrowing-based unification to become finitary. We discuss one of these examples, namely Diffie-Hellman, in the following section.

Variant-preservingness Variant-preservingness is necessary for an eager generation of variants and ensures that whenever an equation is applied, the substitution propagated to the right-hand side of the equation is in normal form. Its actual definition can found in [19]. Let us explain it with an example. Consider the following slightly different version of the exclusive-or theory, where a new sort `Elem` is defined as the basic sort inside an exclusive-or:

```
op _*_ : Msg Msg -> Msg [frozen assoc comm] .
op null : -> Msg .
```

```
sort Elem .
subsort Nonce < Elem < Msg .

eq X:Elem * X:Elem * Y:Msg = Y:Msg [nonexec metadata "variant"] .
eq X:Elem * X:Elem = null [nonexec metadata "variant"] .
eq Y:Msg * null = Y:Msg [nonexec metadata "variant"] .
```

This equational theory does not satisfy the variant-preservingness, since for a term `n(a,r) * n(a,r) * n(b,r') * n(b,r')`, the first equation is the only one applicable but always with a non-normalized substitution. However, in the original definition for exclusive-or of Section 3.2.3, variable `X` is of sort `Msg` and the previous term can be reduced with a normalized substitution by using the substitution `X:Msg` $\mapsto$ `n(a,r) * n(b,r')`.

3.2.7 Some Examples of Admissible Theories

Since any user of the Maude-NPA should write specifications whose algebraic theories are admissible, i.e., satisfy requirements (1)–(7) in Section 3.2.6, it may be useful to illustrate how these requirements are met by several examples. This can give a Maude-NPA user a good intuitive feeling for how to specify algebraic theories that the Maude-NPA currently can handle. For this purpose, we revisit the theories already discussed in Section 3.2.

Let us begin with the theory of Encryption/Decryption:

```
op pk : Name Msg -> Msg [frozen] .
op sk : Name Msg -> Msg [frozen] .

eq pk(A:Name,sk(A:Name,Z:Msg)) = Z:Msg [nonexec metadata "variant"] .
eq sk(A:Name,pk(A:Name,Z:Msg)) = Z:Msg [nonexec metadata "variant"] .
```

In this case $Ax = \emptyset$. It is obvious that in this case the equations E *terminate*, since the *size* of a term as a tree (number of nodes) strictly decreases after the application of any of the above two rules, and therefore it is impossible to have an infinite chain of rewrites with the above equations. It is also easy to check that the equations are *confluent*: by the termination of E this can be reduced to checking confluence of critical pairs, which can be easily discharged by automated tools, or even by hand. Since $Ax = \emptyset$, coherence is a mute point. The equations are also *strongly right irreducible*, because in both cases they are the variable `Z`, and any instance of `Z` by a term that cannot be further simplified by the above equations, obviously cannot be further simplified by hypothesis. Also, the theory is variant-preserving because a term containing several reducible pk-sk symbols can always be simplified using normalized substitutions by reducing the innermost occurrence of the pk-sk symbols.

Let us now consider the Exclusive Or Theory:

```
op _*_ : Msg Msg -> Msg [frozen assoc comm] .
op null : -> Msg .

eq X:Msg * X:Msg * Y:Msg = Y:Msg [nonexec metadata "variant"] .
eq X:Msg * X:Msg = null [nonexec metadata "variant"] .
eq X:Msg * null = X:Msg [nonexec metadata "variant"] .
```

In this case $Ax = AC$. *Termination* modulo AC is again trivial, because the size of a term strictly decreases after applying any of the above equations modulo AC. Because of termination modulo AC, *confluence* modulo AC can be reduced to checking confluence of critical pairs, which can be discharged by standard tools. *Coherence* modulo AC is also easy. As already explained, the first equation has to be added to the second to make it coherent. As also explained above, since the sort `Msg` is biggest possible for the exclusive or operator, the variable `X` in the last equation has the biggest possible sort it can have, and therefore that equation is already coherent, so that there is no need to add an extra equation of the form

```
eq X:Msg * null * Y:Msg = X:Msg * Y:Msg [nonexec]  .
```

because modulo AC such an equation is in fact *an instance* of the third equation (by instantiating `X` to the term `X * Y`). *Strong right irreducibility* is also obvious, since the righthand sides are either variables, or the constant `null`, for which no equations exist. Finally, variant-preservingness of this equational theory was already explained in Section 3.2.6.

Turning now to the Diffie-Hellman theory we have:

```
sorts Name Nonce NeNonceSet Gen Exp Key GenvExp Secret .
subsort Gen Exp < GenvExp .
subsort Name NeNonceSet GenvExp Secret Key < Msg .
subsort Exp < Key .
subsort Nonce < NeNonceSet .
subsorts Name Gen < Public .

op g : -> Gen .
op exp : GenvExp NeNonceSet -> Exp [frozen] .
op _*_ : NeNonceSet NeNonceSet -> NeNonceSet [frozen assoc comm] .

eq exp(exp(W:Gen,Y:NeNonceSet),Z:NeNonceSet)
 = exp(W:Gen, Y:NeNonceSet * Z:NeNonceSet) [nonexec metadata "variant"] .
```

Again, this theory is AC. *Termination* modulo AC is easy to prove by using a polynomial ordering with AC polynomial functions. For example, we can associate to `exp` the polynomial $x+y+1$, and to `*` the polynomial $x+y$. Then the proof of termination becomes just the polynomial inequality $w+y+z+2 > w+y+z+1$. Because of termination modulo AC, *confluence* modulo AC can be reduced to checking the confluence of critical pairs. Here things become interesting. In an untyped setting, the above equation would have a nontrivial overlap with itself (giving rise to a critical pair), by unifying the lefthand side with the subterm `exp(W:Gen,Y:NeNonceSet)`. However, because of the subsort and operator declarations

```
  subsort Gen Exp < GenvExp .
  op exp : GenvExp NeNonceSet -> Exp [frozen] .
```

we see that the order-sorted unification of the subterm `exp(W:Gen,Y:NeNonceSet)` (which has sort `Exp`) and the lefthand side now *fails*, because the sorts `Gen` and `Exp` are mutually exclusive and cannot have any terms in common. Therefore there are no nontrivial critical pairs and the equation is confluent modulo AC. *Coherence* modulo AC is trivially satisfied, because the top operator of the equation (`exp`) is not an AC operator. As in the case of confluence modulo AC, the remaining issue of *strong right irreducibility* becomes particularly interesting in the order-sorted context. Note that in an untyped setting, an instance of the righthand side by applying a substitution whose terms cannot be further simplified *could* itself be simplified. For example, if we consider the untyped righthand side term `exp(W, Y * Z)`, the substitution θ mapping `W` to `exp(Q,X)` and being the identity on `Y` and `Z` is itself irreducible by the equations, but when applied to `exp(W, Y * Z)` makes the corresponding instance reducible by the untyped version of the above equation. However, in the order-sorted setting in which our equation is defined, the equation is indeed strongly right irreducible. This is again because the sorts `Gen` and `Exp` are mutually exclusive and cannot have any terms in common, so that the variable `W:Gen` cannot be instantiated by any term having `gen` as its top operator. Also, the theory is variant-preserving because a term containing several reducible exp symbols can always be simplified using normalized substitutions by reducing the innermost occurrence of the exp symbols.

It may perhaps be useful to conclude this section with an example of an algebraic theory that *does not satisfy* the requirements for a variant equational theory, and thus *cannot* be supported in the current version of Maude-NPA. Consider, the extension of the above exclusive or theory in which we add a *homomorphism* operator and the obvious homomorphism equation:

```
  op h: Msg -> Msg .

  eq h(X:Msg * Y:Msg) = h(X:Msg) * h(Y:Msg) [nonexec medadata "variant"] .
```

The problem now is that the righthand side `h(X) * h(Y)` *fails* to be strongly right-irreducible. For example, the substitution θ mapping `X` to `U * V` and `Y` to `Y` is itself irreducible, but produces the instance `h(U * V) * h(Y)`, which is obviously reducible. Since strong irreducibility is only a *sufficient condition* for narrowing-based equational unification to be finitary, one could in principle hope that this homomorphism example might still have a narrowing-based finitary algorithm[5]. However, the

[5] The fact that an equational theory T does not have a finitary narrowing-based algorithm does not by itself preclude the existence of a finitary unification algorithm obtained by other methods. In fact, the homomorphic theory we have just described does have a finitary unification algorithm

hopes for such a finitary narrowing-based algorithm are dashed to the ground by results in both [6], about the homomorphism theory not having the "finite variant" property, and the variant-based unification methods in [19]. That is why we developed a homomorphism unification algorithm for the Maude-NPA that dodges this problem (see Section 3.2.5). However, the equational theory above, including both variant equations for exclusive-or and a homomorphic operator cannot currently be handled by Maude-NPA, since only a homomorphic equational theory or a variant equational theory are supported, not combinations of boths.

In summary, the main point we wish to emphasize is that the equational theories T for which the current version of Maude-NPA will work properly are one encryption symbol being homomorphic over concatenation or order-sorted theories of the form $T = (\Sigma, E \cup Ax)$ satisfying the admissibility requirements (1)–(7). Under assumptions (1)–(7), T-unification problems are always guaranteed to have a finite number of solutions and the Maude-NPA will find them by narrowing.

As a final *caveat*, if the user specifies a theory T where any of the above conditions (1)–(7) fail, besides the lack of completeness that would be caused by the failure of conditions (2)–(5), a likely consequence of failing to meet conditions (6) or (7) will be that the tool will loop forever trying to solve a unification problem associated with just a single transition step in the symbolic reachability analysis process. However, we are investigating conditions more general than (6) (such as the above-mentioned finite variant property) that will still guarantee that a T-unification problem always has a finite complete set of solutions. Future versions of Maude-NPA will relax condition (6) to allow more general conditions of this kind.

3.3 Protocol Specification

The protocol itself and the intruder capabilities are both specified in the `PROTOCOL-SPECIFICATION` module. They are specified using strands. A *strand*, first defined in [20], is a sequence of positive and negative messages[6] describing a principal executing a protocol, or the intruder performing actions, e.g.,

$$[\ pk(K_B,\ A; N_A)^+,\ pk(K_A, N_A; Z)^-,\ pk(K_B, Z)^+\ ]$$

where a positive node implies sending, and a negative node implies receiving. However, in our tool each strand is divided into the past and future parts, and we keep track of all the variables of sort `Fresh` generated by that concrete strand. That is, the messages to the left of the vertical line were sent or received in the past, whereas

[3]; however this dedicated unification algorithm is not an instance of a generic narrowing-based algorithm. However, as already explained, in the Maude-NPA the theories for which finitary unification is supported are either: (i) order-sorted theories with built-in axioms of commutativity and associativity-commutativity and associativity, communtativity and identity, or (ii) theories modulo such built-in axioms that are confluent, terminating, and coherent modulo Ax, and that are also strongly right irreducible, or (iii) dedicated unification algorithms, such as the one for homomorphic encryption discussed in Section 3.2.5.

[6] We write $m^{\pm}$ to denote m^+ or m^-, indistinctively. We often write $+(m)$ and $-(m)$ instead of m^+ and m^-, respectively.

the messages to the right of the line will be sent or received in the future. Right before the strand, the variables $r_1, \cdots, r_i$ of sort `Fresh` are made explicit, as follows:

$$:: r_1, \ldots, r_i :: [\ {m_1}^{\pm},\ \ldots,\ {m_i}^{\pm} \mid {m_{i+1}}^{\pm},\ \ldots,\ {m_k}^{\pm}\ ]$$

3.3.1 Protocol Specification Variables

We begin by specifying all the variables that are used in this module, together with the sorts of these variables. In the NSPK example, these are

```
vars X Y Z : Msg .
vars r r' : Fresh .
vars A B : Name .
vars N N1 N2 : Nonce .
```

3.3.2 Dolev-Yao Rules

After the variables are specified, the next thing to specify is the intruder, or Dolev-Yao rules. These specify the operations an intruder can perform. An intruder strand consists of a sequence of negative nodes, followed by a single positive node. If the intruder can (non-deterministically) find more than one term as a result of performing one operation (as in deconcatenation), we specify this by separate strands. For the NSPK protocol, we have four operations, encryption with a public key (`pk`), decryption with a private key (`sk`), concatenation (`;`), and deconcatenation.

Encryption with a public key is specified as follows. Note that we use a principal's name to stand for the key. The intruder can encrypt any message using any public key.

```
:: nil:: [ nil | -(X), +(pk(A,X)), nil ]
```

Encryption with the private key is a little different. The intruder can only apply the `sk` operator using his own identity. So we specify the rule as follows.

```
:: nil:: [ nil | -(X), +(sk(i,X)), nil ]
```

Concatenation and deconcatenation are straightforward. If the intruder knows X and Y, he can find $X;Y$. If he knows $X;Y$ he can find X and Y. Since each intruder strand can have at most one positive node, we need to use three rules to specify these:

```
:: nil :: [ nil | -(X), -(Y), +(X ; Y), nil ]
:: nil :: [ nil | -(X ; Y), +(X), nil ]
:: nil :: [ nil | -(X ; Y), +(Y), nil ]
```

The final Dolev-Yao specification looks as follows. Note that our tool requires the use of symbol `STRANDS-DOLEVYAO` as the repository of all the Dolev-Yao strands, and symbol `&` as the union operator for sets of strands. Note, also, that our tool considers that variables are not shared between strands, and thus will appropriately rename them when necessary.

```
eq STRANDS-DOLEVYAO
 = :: nil :: [ nil | -(X), -(Y), +(X ; Y), nil ] &
   :: nil :: [ nil | -(X ; Y), +(X), nil ] &
   :: nil :: [ nil | -(X ; Y), +(Y), nil ] &
   :: nil :: [ nil | -(X), +(sk(i,X)), nil ] &
   :: nil :: [ nil | -(X), +(pk(Ke,X)), nil ]
[nonexec] .
```

3.3.3 Adding/deleting Operations in the Dolev-Yao Strands

Every operation that can be performed by the intruder, and every term that is initially known by the intruder, should have a corresponding intruder rule. For each operation used in the protocol, we should consider whether or not the intruder can perform it, and produce a corresponding intruder strand that describes the conditions under which the intruder can perform it.

For example, suppose that the operation requires the use of exclusive-or. If we assume that the intruder can exclusive-or any two terms in its possession, we would represent this by the following strand:

```
:: nil :: [ nil | -(X), -(Y), X * Y, nil ]
```

If we want to give the intruder the ability to generate his own nonces, we would represent this by the following rule:

```
:: r :: [ nil | +(n(i,r)), nil ]
```

In general, it is a good idea to provide Dolev-Yao rules for all the operation that are defined, unless one is explicit making the assumption that the intruder can *not* perform the operation. It is also *strongly recommended* that operations not used in the protocol should not be provided in Dolev-Yao strands. This is because the tool will attempt to execute these rules, even if they are useless, and so they will negatively affect its performance.

3.3.4 Protocol Rules

In the Protocol Rules section of a specification, we define the messages that are sent and received by the honest principals. We will specify one strand per role. However, since the Maude-NPA analysis supports an arbitrary number of sessions, each strand can be instantiated an arbitrary number of times.

We recall the informal specification of NSPK, as follows:

1. $A \to B : pk(B, A; N_A)$

2. $B \to A : pk(A, N_A; N_B)$

3. $A \to B : pk(B, N_B)$

where N_A and N_B are nonces generated by the respective principals.

In specifying protocol rules it is important to remember to do so from the point of view of the principal executing the role. For example, in NSPK the initiator A starts out by sending her name and a nonce encrypted with B's public key. She gets back something encrypted with her public key, but all she can tell is that it is her nonce concatenated with some other term of sort Nonce. She then encrypts that term of sort Nonce under B's public key and sends it out. In other words, data received by a principal for which the principal could not match its structure must be represented by a variable of sort Msg.

In order to represent this, we represent the construction of A's nonce explicitly as n(A,r), where r is a variable of sort Fresh belonging to A's strand. The nonce she receives, though, is represented by a variable N of sort Nonce, as follows:

```
 :: r ::
 [ nil | +(pk(B,A ; n(A,r))), -(pk(A,n(A,r) ; N)), +(pk(B, N)), nil ]
```

If we wanted to check for type confusion attacks we would replace N of sort Nonce by a variable X of sort Msg (where sort Nonce is a subsort of sort Msg). This implies a bigger search space due to the more general sort of the variable.

In the responder strand, the signs of the messages are reversed. Moreover, the messages themselves are represented differently. B starts out by receiving a name and some nonce encrypted under his key. He creates his own nonce, appends the received nonce to it, encrypts it with the key belonging to the name, and sends it out. He gets back his nonce encrypted under his own key. This is specified as follows:

```
 :: r ::
 [ nil | -(pk(B,A ; N)), +(pk(A, N ; n(B,r))), -(pk(B,n(B,r))), nil ]
```

Note that, as explained above, the point here is to only include things in a strand that a principal executing a strand can actually *verify.* If we say that a principal receives a term of sort Nonce, we assume that the principal has some ability to determine whether something is a nonce, as opposed to some other type of message (perhaps by its length). We do not assume, however, that the principal is able to verify who created that nonce or when. The complete STRANDS-PROTOCOL specification is as follows. We note that in this specification when a principal receives a nonce that she did not create encrypted under her own public key, she is able to decrypt it and determine that is of sort Nonce.

```
eq STRANDS-PROTOCOL =
  :: r ::
  [nil | +(pk(B,A ; n(A,r))), -(pk(A,n(A,r) ; N)), +(pk(B, N)), nil]
  &
  :: r ::
  [nil | -(pk(B,A ; N)), +(pk(A, N ; n(B,r))), -(pk(B,n(B,r))), nil]
[nonexec] .
```

Remember that our tool considers that variables are not shared between strands, and thus will appropriately rename them when necessary.

As a final note, we remark that, if `B` received a message `Z` encrypted under a key he does not know, he would not be able to verify that he received `pk(A,Z)` because he cannot decrypt the message. So the best we could say here is that `A` received some term `Y` of sort `Msg`.

3.3.5 Attack States

The last thing we specify are the *attack states*, which describe the final attack states we are looking for with Maude-NPA. Unlike the case of the Dolev-Yao and protocol strands, we can specify more than one attack state. Thus, we designate each attack state with a natural number.

In Maude-NPA, each state found during the protocol execution (i.e., a backwards search) is represented with four different sections separated by the symbol `||` in the following order: (1) set of current strands, (2) intruder knowledge, (3) sequence of messages, (4) auxiliary data, and (5) never patterns. For instance, the following is a state found for the NSPK protocol:

```
:: nil ::
[ nil |
   -(#0:Msg ; n(b, #1:Fresh)),
   +(n(b, #1:Fresh)), nil]  &
:: #1:Fresh ::
[ nil,
   -(pk(b, a ; #2:Nonce)),
   +(pk(a, #2:Nonce ; n(b, #1:Fresh))) |
   -(pk(b, n(b, #1:Fresh))), nil] )
||
n(b, #1:Fresh) !inI,
pk(b, n(b, #1:Fresh)) inI,
(#0:Msg ; n(b, #1:Fresh)) inI
||
-(#0:Msg ; n(b, #1:Fresh)),
+(n(b, #1:Fresh)),
-(pk(b, n(b, #1:Fresh)))
||
nil
||
nil
```

The intruder knowledge represents what the intruder knows (symbol `_inI`) or doesn't know (symbol `_!inI`) at each state. However, the symbol `_!inI` represents that it is not known now but it would be known in the future. The set of current strands indicates how advanced each strand is in the execution process (by the placement of the bar), and gives partial substitutions for the messages in each strand. Note that the set of strands and the intruder knowledge *grow along with* the backwards reachability search, in one case by introducing more protocol or intruder strands, and in the other case by introducing more positive knowledge of the intruder (e.g., `M inI`) or by transforming positive into negative knowledge due to the backwards execution (e.g., `M inI` ⇒ `M !inI`). The sequence of messages, which is nil at the beginning gives the actual sequence of messages passed. This also grows as the backwards search continues, and gives a complete description of an attack when an initial state is reached. This part is intended for the benefit of the user, and is not actually used in the backward search. The fifth part contains the never patterns associated to this state, and are explained in more detail in Section 3.3.6. Finally, the fourth part is used to store information about the search space that the tool creates to help manage its search. It does not provide any information about the attack itself, and is currently only displayed by the tool to help in debugging. More information about debugging facilities can be found in Appendix D.

The user can specify only the first two parts of an attack state: the set of strands expected to appear in the attack, and the intruder knowledge. The other two sections must have just the empty symbol `nil`.

For NSPK, the standard attack is represented as follows:

```
eq ATTACK-STATE(0) =
   :: r ::
   [ nil,
      -(pk(b,a ; N)),
      +(pk(a, N ; n(b,r))),
      -(pk(b,n(b,r))) |
      nil ]
   ||
   n(b,r) inI
   ||
   nil
   ||
   nil
   ||
   nil
 [nonexec] .
```

where we require the intruder to have learned the nonce generated by Bob, and thus we have to include Bob's strand in the attack in order to describe such specific nonce `n(b,r)`.

We can also specify inequalities (the condition that a term not be equal to something) in the intruder knowledge section. For example, suppose that we want to specify that a responder executes a strand, apparently with an initiator `a`, but the nonce received is not generated by `a`. This would be done as follows:

```
eq ATTACK-STATE(0) =
   :: r ::
   [ nil,
      -(pk(b,a ; N)),
      +(pk(a, N ; n(b,r))),
      -(pk(b,n(b,r))) |
      nil ]
   ||
   N != n(a,r')
   ||
   nil
   ||
   nil
   ||
   nil
 [nonexec] .
```

where t `!=` s means that for any ground substitution θ applicable to t and s, $\theta(t)$ cannot be equal to $\theta(s)$ modulo the equational theory. Note that, since a is a constant and r' is a variable of the special sort `Fresh`, `N != n(a,r')` means that `N` cannot be of the form `n(a,r')`.

In summary, we note the following conditions on attack state specifications:

1. Strands in the attack state must have the bar at the end.

2. If more than one strand appears in the attack state, they must be separated by the `&` symbol. If more than one term appears in the intruder knowledge, they must be separated by commas. If no strands appear, or no terms appear, the `empty` symbol is used, in the strands or intruder knowledge sections, respectively, e.g.,

```
eq ATTACK-STATE(0) =
  :: r ::
  [ nil,
     -(pk(b,a ; N)),
     +(pk(a, N ; n(b,r))),
     -(pk(b,n(b,r))) |
     nil ]
  || empty
  || nil
  || nil
  || nil
[nonexec] .
```

3. The items that can appear in the intruder knowledge may include not only terms known by the intruder, but also inequality conditions on terms.

4. The two fields after the intruder knowledge must always be `nil`. These are fields that contain information that is built up in the backwards search, but is empty in the final attack state.

5. The last field would usually be `nil` except if a never pattern is included, explained in the next section.

3.3.6 Attack States With Excluded Patterns: Never Patterns

It is often desirable to exclude certain patterns from transition paths leading to an attack state. For example, one may want to determine whether or not authentication properties have been violated, e.g., whether it is possible for a responder strand to appear without the corresponding initiator strand. For this there is an optional additional field in the attack state containing the never patterns.

Here is how we would specify an initiator strand without a responder in the NSPK protocol:

```
eq ATTACK-STATE(1) =
  :: r ::
  [ nil,
     -(pk(b,a ; N)),
     +(pk(a, N ; n(b,r))),
     -(pk(b,n(b,r))) |
     nil ]
  || empty
  || nil
  || nil
  || never(
     *** for authentication
     :: r' ::
     [ nil |
        +(pk(b,a ; N)),
        -(pk(a, N ; n(b,r))),
        +(pk(b,n(b,r))), nil ]
     & S:StrandSet
     || K:IntruderKnowledge
     )
  [nonexec] .
```

Note that the never pattern does not contain the extra fields included in an attack pattern and only strands and intruder knowledge are available. Note that variables of the regular strands or the regular intruder knowledge may appear in the never pattern as a way to differentiate and constrain the never pattern. For instance, the variable `r'` in the never pattern is not an error, since the regular strand in the attack state is the initiator strand, which generates variable `r`, and the strand in the never pattern is a pattern that must be valid for any responder strand. Any responder strand would generate his variable `r'`.

If we want to restrict the existence of a responder strand even more, so that no *partial responder strand* can show up, we must include a second never pattern ending in a positive message of the strand (since partial strands will always end in a positive message and represent incomplete strands):

```
eq ATTACK-STATE(1) =
  :: r ::
  [ nil,
    -(pk(b,a ; N)),
    +(pk(a, N ; n(b,r))),
    -(pk(b,n(b,r))) |
    nil ]
 || empty
 || nil
 || nil
 || never(
    *** for authentication
    (:: r' ::
    [ nil |
       +(pk(b,a ; N)),
       -(pk(a, N ; n(b,r))),
       +(pk(b,n(b,r))), nil ]
    & S:StrandSet
    || K:IntruderKnowledge)
    *** for authentication
    (:: r' ::
    [ nil |
       +(pk(b,a ; N)), nil ]
    & S:StrandSet
    || K:IntruderKnowledge)
    )
 [nonexec] .
```

Note that variable names used in different never patterns have no effect, since each never pattern is checked independently. The tool will now look for all paths in which the intruder strand is executed, but no (partial) responder strand is running.

It is also possible to use never patterns to specify negative conditions on terms or strands. Suppose we want to ask if it is possible for a responder in the NSPK protocol to execute a session of the protocol, apparently with an initiator, but the nonce received was not the initiator's (represented by `n(a,r')`). This would be done as follows:

```
eq ATTACK-STATE(2) =
 :: r ::
 [ nil,
    -(pk(b,a ; N)),
    +(pk(a, N ; n(b,r))),
    -(pk(b,n(b,r))) |
    nil ]
 || empty
 || nil
 || nil
 || never(
    *** for authentication
    (:: r' ::
    [ nil |
       -(pk(b,a ; n(a,r'))),
       +(pk(a, n(a,r') ; n(b,r))),
       -(pk(b,n(b,r))), nil ]
    & S:StrandSet
    || K:IntruderKnowledge)
    )
 [nonexec] .
```

We note that it is possible to put more than one never pattern in a search space, but then each such pattern must be contained in a pair of parentheses, e.g.,

```
never(
( ... State 1 ... )
( ... State 2 ... )
)
```

Never patterns can also be used to cut the down the search space. Suppose, for example, that one finds in the above search that a number of states are encountered in which the intruder encrypts two nonces, but they never seem to provide any useful information. One can reduce the search space by ruling out that intruder behavior with the following never pattern:

```
eq ATTACK-STATE(1) =
 :: r ::
 [ nil,
    -(pk(b,a ; N)),
    +(pk(a, N ; n(b,r))),
    -(pk(b,n(b,r))) |
    nil ]
 || empty
 || nil
 || nil
 || never(
    *** cut down search for two nonces
    :: nil ::
    [ nil |
       -(N1 ; N2),
       +(pk(A, N1 ; N2)), nil ]
    & S:StrandSet
    || K:IntruderKnowledge
    )
 [nonexec] .
```

Note that adding `Never` patterns to reduce the search space, as distinguished from their use for verifying *authentication* properties, means that failure to find an attack does not necessarily mean that the protocol is secure. It simply means that any attack against the security property specified in the attack state must use at least one strand that is specified in the set of never patterns.

There are several things about the never patterns that should be noted:

1. The bar in any strand in the never pattern should be at the beginning of the strand. If it is not, we will enforce it.

2. The first two fields must end in variables of type `Strandset` and `Intruderknowledge`, respectively.

3. More than one never pattern can be used in an attack state. Each one must be delimited by its own set of parentheses.

For a good example of the use of never patterns, which makes the Maude-NPA search considerably more efficient without compromising the completeness of the reachability analysis, we refer the reader to the analysis of the Diffie-Hellman protocol in Section 5.3.

3.4 Grammars

The Maude-NPA's ability to reason effectively about low-level algebraic properties is a result of its combination of symbolic reachability analysis using narrowing, together with its grammar-based techniques for reducing the size of the search space. Here we briefly explain how grammars work as a state space reduction technique and refer the reader to [26, 12] for further details.

Automatically generated grammars $\langle G_1, \ldots, G_m \rangle$ represent unreachability information (or co-invariants), i.e., typically infinite sets of states unreachable for the intruder. That is, given a message m and an automatically generated grammar G, if $m \in G$, then there is no initial state St_{init} and substitution θ such that the intruder knowledge of St_{init} contains the fact $\theta(m)$ `!inI`, i.e., the intruder is not able to learn message m. These automatically generated grammars are very important in our framework, since in the best case they can reduce the infinite search space to a finite one, or, at least, can drastically reduce the search space.

Unlike the grammars used in NPA, described in [26], and the version of Maude-NPA described in [12], in which initial grammars needed to be specified by the user, Maude-NPA now generates initial grammars automatically. Each initial grammar consists of a single seed term of the form $C \mapsto f(X_1, \cdots, X_n) {\in} \mathcal{L}$, where f is an operator symbol from the protocol specification, the X_i are variables, and C is either empty or consists of the single constraint (X_i `inI`) (similar to expression X_i `inI` but used in a different context). However, Maude-NPA provides features to control such automatically generated grammars, e.g., adding more seed terms. Appendix B gives a more detailed description of grammars and its features in the Maude-NPA.

4 Maude-NPA Commands for Attack Search

The commands `run`, `summary`, and `initials` are the tool's commands for attack search. They are invoked by reducing them in Maude, that is, by typing `red` followed by the command, followed by a space and a period. To use them we must specify the attack state we are searching for, and the number of backwards reachability steps we want to compute, e.g.,

```
run(0,10)
```

tells Maude-NPA to construct the backwards reachability tree up to depth 10 for the attack state designated with natural number 0. The command `run` yields the set of states found in the leaves of the backwards reachability tree of the specified depth that has been generated. When the user is not interested in the current states of the reachability tree, he/she can use the command `summary`, which outputs just the number of states found in the leaves of the reachability tree and how many of those are initial states, i.e., solutions to the attack. For instance, when we give the reduce command `summary(0,2)` in Maude as below for the NSPK example, it returns:

```
red summary(0,2) .
result Summary: States>> 6 Solutions>> 0
```

The initial state representing the standard NSPK attack is found in 7 steps.

```
red summary(0,7) .
result Summary: States>> 4 Solutions>> 1
```

We also provide a slightly different version of the `run` command that outputs only the initial states, instead of all the leaves. Thus, if we type

```
red initials(0,7) .
```

for the NSPK example our tool outputs the attack[7]:

```
Maude> red initials(0,7) .
< 1 . 5 . 2 . 5 . 2 . 3 . 3 . 1 > (
:: nil ::
[ nil |
   -(pk(i, n(b, #1:Fresh))),
   +(n(b, #1:Fresh)), nil]  &
:: nil ::
[ nil |
   -(pk(i, a ; n(a, #0:Fresh))),
   +(a ; n(a, #0:Fresh)), nil]  &
:: nil ::
[ nil |
   -(n(b, #1:Fresh)),
   +(pk(b, n(b, #1:Fresh))), nil]  &
:: nil ::
[ nil |
   -(a ; n(a, #0:Fresh)),
   +(pk(b, a ; n(a, #0:Fresh))), nil]  &
:: #0:Fresh ::
[ nil |
   +(pk(i, a ; n(a, #0:Fresh))),
   -(pk(a, n(a, #0:Fresh) ; n(b, #1:Fresh))),
```

[7] Note that Maude-NPA associates an identifier, e.g. 1.5.2.7.1.4.3.1, to each state generated by the tool. These identifiers are for internal use and are not described in this manual.

```
   +(pk(i, n(b, #1:Fresh))), nil]  &
:: #1:Fresh ::
[ nil |
   -(pk(b, a ; n(a, #0:Fresh))),
   +(pk(a, n(a, #0:Fresh) ; n(b, #1:Fresh))),
   -(pk(b, n(b, #1:Fresh))), nil] )
||
pk(a, n(a, #0:Fresh) ; n(b, #1:Fresh)) !inI,
pk(b, n(b, #1:Fresh)) !inI,
pk(b, a ; n(a, #0:Fresh)) !inI,
pk(i, n(b, #1:Fresh)) !inI,
pk(i, a ; n(a, #0:Fresh)) !inI,
n(b, #1:Fresh) !inI,
(a ; n(a, #0:Fresh)) !inI
||
+(pk(i, a ; n(a, #0:Fresh))),
-(pk(i, a ; n(a, #0:Fresh))),
+(a ; n(a, #0:Fresh)),
-(a ; n(a, #0:Fresh)),
+(pk(b, a ; n(a, #0:Fresh))),
-(pk(b, a ; n(a, #0:Fresh))),
+(pk(a, n(a, #0:Fresh) ; n(b, #1:Fresh))),
-(pk(a, n(a, #0:Fresh) ; n(b, #1:Fresh))),
+(pk(i, n(b, #1:Fresh))),
-(pk(i, n(b, #1:Fresh))),
+(n(b, #1:Fresh)),
-(n(b, #1:Fresh)),
+(pk(b, n(b, #1:Fresh))),
-(pk(b, n(b, #1:Fresh)))
||
nil
||
nil
```

This corresponds to the following textbook version of the attack:

1. $A \to I : pk(I, A; N_A)$
2. $I_A \to B : pk(B, A; N_A)$
3. $B \to A : pk(A, N_A; N_B)$, intercepted by I;
4. $I \to A : pk(A, N_A; N_B)$
5. $A \to I : pk(I, N_B)$
6. $I_A \to B : pk(B, N_B)$

It is also possible to generate an unbounded search by specifying the second argument of `run`, `initials`, or `summary` as `unbounded`. In that case, the tool will run until it has shown that all the paths it has found either begin in initial states or in unreachable ones. This check may terminate in finite time, but in some cases may run forever.

We demonstrate with NSPK:

```
red summary(0,unbounded) .
result Summary: States>> 1 Solutions>> 1
```

This tells us, that Maude-NPA terminated with only one attack. If we want to see what that attack is, we reduce the command `run(0,unbounded)` to get the attack displayed above.

4.1 Needham-Schroeder-Lowe: A Secure Protocol

If we consider Lowe's fix of the Needham-Schroeder protocol, Maude-NPA is able to prove that the protocol is secure, that is, no initial state is found and the search space is finite.

We recall the informal specification of NSL, as follows:

1. $A \to B : pk(B, A; N_A)$
2. $B \to A : pk(A, N_A; N_B; B)$
3. $A \to B : pk(B, N_B)$

Note that the only change in NSL protocol w.r.t. the NSPK protocol is that the responder B sends both nonces together with his name, instead of sending just both nonces.

The protocol is specified in Maude-NPA as follows, keeping the sort and operator declarations as well as the intruder strands of the NSPK protocol.

```
eq STRANDS-PROTOCOL =
  :: r ::
  [nil | +(pk(B,A ; n(A,r))), -(pk(A,n(A,r) ; N ; B)), +(pk(B, N)), nil]
  &
  :: r ::
  [nil | -(pk(B,A ; N)), +(pk(A, N ; n(B,r) ; B)), -(pk(B,n(B,r))), nil]
[nonexec] .
```

The attack pattern representing the intruder able to learn the responder's nonce (similar to the NSPK attach pattern) is as follows:

```
  eq ATTACK-STATE(0)
   = :: r ::
     [ nil,
        -(pk(b,a ; N)),
        +(pk(a, N ; n(b,r) ; b)),
        -(pk(b,n(b,r))) |
        nil ]
     ||
     n(b,r) inI
     ||
     nil
     ||
     nil
     ||
     nil
  [nonexec] .
```

And the search space associated to this protocol is as follows:

```
reduce in MAUDE-NPA : summary(1) .
result Summary: States>> 4 Solutions>> 0

reduce in MAUDE-NPA : summary(2) .
result Summary: States>> 7 Solutions>> 0

reduce in MAUDE-NPA : summary(3) .
result Summary: States>> 6 Solutions>> 0

reduce in MAUDE-NPA : summary(4) .
result Summary: States>> 2 Solutions>> 0

reduce in MAUDE-NPA : summary(5) .
result Summary: States>> 0 Solutions>> 0
```

5 More Examples

In the following, we describe how the Maude-NPA analyzes several examples whose algebraic properties have already been defined above.

5.1 Needham-Schroeder-Lowe with Homomorphic Encryption

When we consider the secure Needham-Schroeder-Lowe protocol of Section 4.1 and make encryption homomorphic over concatenation, the protocol becomes insecure. In order to be able to use the homomorphic unification available in Maude-NPA, the encryption operator must swap its arguments in contrast to the protocol definition of Section 4.1. That is, the informal specification of NSL is as follows:

1. $A \to B : pk(N_A; A, B)$
2. $B \to A : pk(N_A; N_B; B, A)$
3. $A \to B : pk(N_B, B)$

There are a number of ways in which either A or B can be tricked into believing that they have successfully completed a run of the protocol with another, when in fact this has not happened. Here is one of the simplest:

1. $I_A \to B : pke(N_I; A, B)$
2. $B \to I_A : pke(N_I; N_B; B, A)$

   This message is intercepted by the intruder, who, thanks to the homomorphic property, is able to extract $pke(N_B, A)$. He uses this to initiate the protocol with A, posing as B. Again the intruder uses the homomorphic property to build the following message:

3. $I_B \to A : pke(N_B; B, A)$
4. $A \to I_B : pke(N_A; N_B; A, B)$

   The intruder is now able to extract $pke(N_B, B)$ and use it to complete its impersonation of A to B.
5. $I_A \to B : pke(N_B, B)$.

The protocol is specified in Maude-NPA as follows. First the sort and operator declarations, similar to the NSPK and NSL protocols.

```
sorts Name Nonce Key .
subsort Name Nonce Key < Msg .
subsort Name < Key .
subsort Name < Public .

op pk : Msg Key -> Msg [frozen] .

op n : Name Fresh -> Nonce [frozen] .

op a : -> Name . --- Alice
op b : -> Name . --- Bob
op i : -> Name . --- Intruder

op _;_ : Msg  Msg  -> Msg [gather (e E) frozen] .
```

The equational property was specified in Section 3.2.5.

```
eq pk(X:Msg ; Y:Msg, K:Key) = pk(X:Msg, K:Key) ; pk(Y:Msg, K:Key)
     [nonexec label homomorphism metadata "builtin-unify"] .
```

The Dolev-Yao intruder capabilities here reflect the cancellation of encryption and decryption explicitly.

```
vars X Y : Msg .
vars A B : Name .
var Ke : Key .
var r : Fresh .

eq STRANDS-DOLEVYAO
 = :: nil :: [ nil | -(X), -(Y), +(X ; Y), nil ] &
   :: nil :: [ nil | -(X ; Y), +(X), nil ] &
   :: nil :: [ nil | -(X ; Y), +(Y), nil ] &
   :: nil :: [ nil | -(X), +(pk(X,Ke)), nil ] &
   :: nil :: [ nil | -(pk(X,i)), +(X), nil ] &
   :: r ::   [ nil | +(n(i,r)), nil ] &
   :: nil :: [ nil | +(A), nil ]
[nonexec] .
```

The protocol is described as follows (very similar to the NSL protocol).

```
eq STRANDS-PROTOCOL
 = :: r ::
   [ nil | +(pk(A ; n(A,r), B)),
           -(pk(n(A,r) ; NB ; B, A)),
           +(pk(NB, B)), nil ]
   &
   :: r ::
   [ nil | -(pk(A ; NA, B)),
           +(pk(NA ; n(B,r) ; B, A)),
           -(pk(n(B,r), B)), nil ]
[nonexec] .
```

The attack pattern representing the intruder able to learn the responder's nonce (similar to the NSPK attach pattern) is as follows:

```
eq ATTACK-STATE(0)
 = :: r ::
   [ nil,
      -(pk(a ; N, b)),
      +(pk(N ; n(b,r) ; b, a)),
      -(pk(n(b,r), b)) |
      nil ]
   ||
   n(b,r) inI
   ||
   nil
   ||
   nil
   ||
   nil
[nonexec] .
```

The following initial state from the previous attack pattern is found in seven steps, while the search space being finite is found after thirteen backwards reachability steps[8].

```
(< 1 . 2 . 9 . 12 . (2{1}) . 6 . 1 . 1 > (
:: nil ::
[ nil |
   -(pk(i, b)),
   -(pk(n(b, #1:Fresh), b)),
   +(pk(i, b) ; pk(n(b, #1:Fresh), b)), nil]  &
:: nil ::
[ nil |
   -(pk(n(b, #1:Fresh), i)),
   +(n(b, #1:Fresh)), nil]  &
:: nil ::
```

[8] The keyword `generatedByIntruder` in the actual message list exchanged by the principals is included only for debugging purposes and does not imply any exchange between principals.

```
[ nil |
   -(pk(n(b, #1:Fresh), i) ; pk(n(b, #2:Fresh), i) ; pk(b, i)),
   +(pk(n(b, #1:Fresh), i)), nil]  &
:: #1:Fresh ::
[ nil |
   -(pk(a ; n(a, #0:Fresh), b)),
   +(pk(n(a, #0:Fresh) ; n(b, #1:Fresh) ; b, a)),
   -(pk(n(b, #1:Fresh), b)), nil]  &
:: #2:Fresh ::
[ nil |
   -(pk(i ; n(b, #1:Fresh), b)),
   +(pk(n(b, #1:Fresh) ; n(b, #2:Fresh) ; b, i)), nil]  &
:: #0:Fresh ::
[ nil |
   +(pk(a ; n(a, #0:Fresh), b)),
   -(pk(n(a, #0:Fresh) ; n(b, #1:Fresh) ; b, a)),
   +(pk(n(b, #1:Fresh), b)), nil] )
||
pk(i, b) !inI,
pk(n(b, #1:Fresh), b) !inI,
pk(n(b, #1:Fresh), i) !inI,
pk(a ; n(a, #0:Fresh), b) !inI,
pk(n(a, #0:Fresh) ; n(b, #1:Fresh) ; b, a) !inI,
pk(n(b, #1:Fresh) ; n(b, #2:Fresh) ; b, i) !inI,
n(b, #1:Fresh) !inI,
(pk(i, b) ; pk(n(b, #1:Fresh), b)) !inI
||
+(pk(a ; n(a, #0:Fresh), b)),
-(pk(a ; n(a, #0:Fresh), b)),
+(pk(n(a, #0:Fresh) ; n(b, #1:Fresh) ; b, a)),
generatedByIntruder(pk(i, b)),
-(pk(n(a, #0:Fresh) ; n(b, #1:Fresh) ; b, a)),
+(pk(n(b, #1:Fresh), b)),
-(pk(i, b)),
-(pk(n(b, #1:Fresh), b)),
+(pk(i, b) ; pk(n(b, #1:Fresh), b)),
-(pk(i ; n(b, #1:Fresh), b)),
+(pk(n(b, #1:Fresh) ; n(b, #2:Fresh) ; b, i)),
-(pk(n(b, #1:Fresh), i) ; pk(n(b, #2:Fresh), i) ; pk(b, i)),
+(pk(n(b, #1:Fresh), i)),
-(pk(n(b, #1:Fresh), i)),
+(n(b, #1:Fresh)),
-(pk(n(b, #1:Fresh), b))
||
nil
||
nil
```

5.2 Needham-Schroeder-Lowe with Exclusive-or

Similarly to the previous section, if we replace concatenation by exclusive-or, the protocol becomes insecure. The informal specification of NSL is as follows:

1. $A \to B : pk(B, N_A; A)$
2. $B \to A : pk(A, N_A; N_B * B)$
3. $A \to B : pk(B, N_B)$

The attack is performed as follows:

1. $A \to I_B : pk(i, N_A; A)$
   The intruder extracts the nonce from the initiator and starts another session with the responder.

2. $I_A \to B : pk(B, N_A; A)$

3. $B \to A : pk(A, N_A; N_B * B)$
   The initiator is expecting a message of the form $pk(A, N_A; N_I * I)$ where N_I is unknown. But the message $pk(A, N_A; N_B * B)$ can also be interpreted as $pk(A, N_A; N_B * B * i * i)$ where $N_I = N_B * B * i$.

4. $A \to I_B : pk(i, N_B * B * i)$
   The intruder is able to extract N_B by decrypting and composing the message with i and B, which are known to the intruder.

The protocol is specified in Maude-NPA as follows. First the sort and operator declarations, similar to the NSPK and NSL protocols.

```
sorts Name Nonce NNSet .
subsort Name Nonce NNSet < Msg .
subsort Name < Public .
subsort Name Nonce < NNSet .

op pk : Name Msg -> Msg [frozen] .
op sk : Name Msg -> Msg [frozen] .

op _;_ : Msg Msg -> Msg [gather (e E) frozen] .

op n : Name Fresh -> Nonce [frozen] .

op a : -> Name . --- Alice
op b : -> Name . --- Bob
op i : -> Name . --- Intruder

op _*_ : NNSet NNSet -> NNSet [assoc comm frozen] .
op null : -> NNSet .
```

The equational properties are the exclusive-or and the cancellation of encryption and decryption.

```
*** Encryption/Decryption Cancellation
eq pk(A:Name,sk(A:Name,Z:Msg)) = Z:Msg [metadata "variant"] .
eq sk(A:Name,pk(A:Name,Z:Msg)) = Z:Msg [metadata "variant"] .

*** Exclusive or properties
eq XN:NNSet * XN:NNSet = null                [metadata "variant"] .
eq XN:NNSet * XN:NNSet * YN:NNSet = YN:NNSet [metadata "variant"] .
eq XN:NNSet * null = XN:NNSet                [metadata "variant"] .
```

The Dolev-Yao intruder capabilities here reflect the cancellation of encryption and decryption explicitly.

```
vars X Y : Msg .
vars A B : Name .
vars XN YN : NNSet .
var r : Fresh .

eq STRANDS-DOLEVYAO
 = :: nil :: [ nil | -(X), -(Y), +(X ; Y), nil ] &
   :: nil :: [ nil | -(X ; Y), +(X), nil ] &
   :: nil :: [ nil | -(X ; Y), +(Y), nil ] &
   :: nil :: [ nil | -(XN), -(YN), +(XN * YN), nil ] &
   :: nil :: [ nil | -(X), +(sk(i,X)), nil ] &
   :: nil :: [ nil | -(X), +(pk(A,X)), nil ] &
   :: nil :: [ nil | +(null), nil ] &
   :: r   :: [ nil | +(n(i,r)), nil ] &
   :: nil :: [ nil | +(A), nil ]
```

The protocol is described as follows (very similar to the NSL protocol).

```
eq STRANDS-PROTOCOL
= :: r ::  *** Bob ***
  [nil | +(pk(B, n(A,r) ; A)),
         -(pk(A, n(A,r) ; B * YN)),
         +(pk(B, YN)), nil]
  &
  :: r' :: *** Alice ***
  [nil | -(pk(B, XN ; A)),
         +(pk(A, XN ; B * n(B,r'))),
         -(pk(B,n(B,r'))), nil]
```

The attack pattern representing the intruder able to learn the responder's nonce (similar to the NSPK attach pattern) is as follows:

```
eq ATTACK-STATE(0)
 = :: r' :: *** Alice ***
   [nil,
     -(pk(b, XN ; a)),
     +(pk(a, XN ; b * n(b,r'))),
     -(pk(b, n(b,r'))) |
     nil]
   ||
   n(b,r') inI, empty
   ||
   nil
   ||
   nil
   ||
   nil
[nonexec] .
```

The following initial state from the previous attack pattern is found in eight steps, while the search space being finite is found after eleven backwards reachability steps.

```
< 1 . 11 . 3 . 23 . 37 . 5 . 3 . 2 . 1 > (
:: nil ::
[ nil |
   -(pk(i, n(a, #0:Fresh) ; a)),
   +(n(a, #0:Fresh) ; a), nil]  &
:: nil ::
[ nil |
   -(pk(i, b * i * n(b, #1:Fresh))),
   +(b * i * n(b, #1:Fresh)), nil]  &
:: nil ::
[ nil |
   -(n(a, #0:Fresh) ; a),
   +(pk(b, n(a, #0:Fresh) ; a)), nil]  &
:: nil ::
[ nil |
   -(n(b, #1:Fresh)),
   +(pk(b, n(b, #1:Fresh))), nil]  &
:: nil ::
[ nil |
   -(b * i),
   -(b * i * n(b, #1:Fresh)),
   +(n(b, #1:Fresh)), nil]  &
:: #0:Fresh ::
[ nil |
   +(pk(i, n(a, #0:Fresh) ; a)),
   -(pk(a, n(a, #0:Fresh) ; b * n(b, #1:Fresh))),
   +(pk(i, b * i * n(b, #1:Fresh))), nil]  &
:: #1:Fresh ::
[ nil |
   -(pk(b, n(a, #0:Fresh) ; a)),
   +(pk(a, n(a, #0:Fresh) ; b * n(b, #1:Fresh))),
   -(pk(b, n(b, #1:Fresh))), nil] )
||
pk(a, n(a, #0:Fresh) ; b * n(b, #1:Fresh)) !inI,
pk(b, n(a, #0:Fresh) ; a) !inI,
pk(b, n(b, #1:Fresh)) !inI,
pk(i, n(a, #0:Fresh) ; a) !inI,
pk(i, b * i * n(b, #1:Fresh)) !inI,
(n(a, #0:Fresh) ; a) !inI,
n(b, #1:Fresh) !inI,
(b * i) !inI,
(b * i * n(b, #1:Fresh)) !inI
||
+(pk(i, n(a, #0:Fresh) ; a)),
-(pk(i, n(a, #0:Fresh) ; a)),
+(n(a, #0:Fresh) ; a),
-(n(a, #0:Fresh) ; a),
+(pk(b, n(a, #0:Fresh) ; a)),
generatedByIntruder(b * i),
-(pk(b, n(a, #0:Fresh) ; a)),
+(pk(a, n(a, #0:Fresh) ; b * n(b, #1:Fresh))),
-(pk(a, n(a, #0:Fresh) ; b * n(b, #1:Fresh))),
+(pk(i, b * i * n(b, #1:Fresh))),
-(pk(i, b * i * n(b, #1:Fresh))),
+(b * i * n(b, #1:Fresh)),
-(b * i),
-(b * i * n(b, #1:Fresh)),
+(n(b, #1:Fresh)),
-(n(b, #1:Fresh)),
+(pk(b, n(b, #1:Fresh))),
-(pk(b, n(b, #1:Fresh)))
||
nil
||
nil
```

5.3 Diffie-Hellman Protocol

The informal textbook-level description of the protocol is as follows.

1. $A \to B : A\ ;\ B\ ;\ g^{N_A}$
2. $B \to A : A\ ;\ B\ ;\ g^{N_B}$
3. $A \to B : e(g^{N_B \cdot N_A}, secret)$

The initiator A starts out by sending her name, the name of B, and g raised to the NA where g is the generator of the Diffie-Hellman group being used, and NA is a nonce. She is supposed to get back the concatenation of her name, the name of B, and a generator g raised to B's nonce NB. However, all she can tell is that she receives the two names and an exponentiation, called XE. Then, she replies by encrypting a secret (to be shared with B) with XE raised to her nonce NA.

The sorts used in this protocol are as follows, where sorts GenvExp, Gen, and Exp have been explained in Section 3.2.4 above.

```
  sorts Name Nonce NeNonceSet Gen Exp Key GenvExp Secret .
  subsort Gen Exp < GenvExp .
  subsort Name NeNonceSet GenvExp Secret Key < Msg .
  subsort Exp < Key .
  subsort Name < Public .
  subsort Gen < Public .
```

The operations used are as follows, where operators g and exp have been explained in Section 3.2.4 above.

```
  --- Secret
  op sec : Name Fresh -> Secret [frozen] .
  --- Nonce operator
  op n : Name Fresh -> Nonce [frozen] .
  --- Intruder
  ops a b i : -> Name .
  --- Encryption
  op e : Key Msg -> Msg [frozen] .
  op d : Key Msg -> Msg [frozen] .
  --- Exp
  op exp : GenvExp NeNonceSet -> Exp [frozen] .
  --- Gen
```

```
op g : -> Gen .
--- NeNonceSet
subsort Nonce < NeNonceSet .
op _*_ : NeNonceSet NeNonceSet -> NeNonceSet [frozen assoc comm] .
--- Concatenation
op _;_ : Msg Msg -> Msg [frozen gather (e E)] .
```

The algebraic equations besides associative-commutative are specified as follows:

```
eq exp(exp(W:Gen,Y:NeNonceSet),Z:NeNonceSet)
 = exp(W:Gen, Y:NeNonceSet * Z:NeNonceSet) [metadata "variant"] .
eq e(K:Key,d(K:Key,M:Msg)) = M:Msg [metadata "variant"] .
eq d(K:Key,e(K:Key,M:Msg)) = M:Msg [metadata "variant"] .
```

The Dolev-Yao intruder capabilities associated to these operation symbols are described as follows.

```
vars M M1 M2 : Msg .
vars NS1 NS2 : NeNonceSet .
var GE : GenvExp .
vars A B : Name .
var Ke : Key .
var r : Fresh .

eq STRANDS-DOLEVYAO =
   :: nil :: [ nil | -(M1 ; M2), +(M1), nil ] &
   :: nil :: [ nil | -(M1 ; M2), +(M2), nil ] &
   :: nil :: [ nil | -(M1), -(M2), +(M1 ; M2), nil ] &
   :: nil :: [ nil | -(Ke), -(M), +(e(Ke,M)), nil ] &
   :: nil :: [ nil | -(Ke), -(M), +(d(Ke,M)), nil ] &
   :: nil :: [ nil | -(NS1), -(NS2), +(NS1 * NS2), nil ] &
   :: nil :: [ nil | -(GE), -(NS), +(exp(GE,NS)), nil ] &
   :: r ::   [ nil | +(n(i,r)), nil ] &
   :: nil :: [ nil | +(g), nil ] &
   :: nil :: [ nil | +(A), nil ]
[nonexec] .
```

The informal textbook-level description above is specified in Maude-NPA as follows, taking into account that a received exponentiation that is unknown to a principal is represented by a variable. The strand for principal A is:

```
:: r,r’ ::
[nil | +(A ; B ; exp(g,n(A,r))),
       -(A ; B ; XE),
       +(e(exp(XE,n(A,r)),sec(A,r’))), nil]
```

Note that A uses two fresh variables, one for the nonce and another for the secret data. And the strand for principal B is:

```
:: r ::
[nil | -(A ; B ; XE),
       +(A ; B ; exp(g,n(B,r))),
       -(e(exp(XE,n(B,r)),Sr)), nil]
```

The attack state is represented by the following pattern, which states that only the strand of `B` is required to appear in the possible initial state, and that no intruder knowledge is required. Moreover, for authentication purposes, the initiator strand is avoided using a never pattern:

```
eq ATTACK-STATE(0)
 = :: r ::
   [nil, -(a ; b ; XE),
         +(a ; b ; exp(g,n(b,r))),
         -(e(exp(XE,n(b,r)),sec(a,r'))) | nil]
   || empty
   || nil
   || nil
   || never
   *** Pattern for authentication
   (:: R:FreshSet ::
   [nil | +(a ; b ; XE),
          -(a ; b ; exp(g,n(b,r))),
          +(e(YE,sec(a,r'))), nil]
    & S:StrandSet || K:IntruderKnowledge)
[nonexec] .
```

The search terminates in twelve backwards narrowing steps and two attacks are found. We list the first[9]:

```
result IdSystemSet: (< (1[2]) . 6 . 4 . 3 . 7 . 7 . 1 . 3 . 2 . 6 . 6 . 1 > (
:: nil ::
[ nil |
   -(a),
   -(b ; exp(g, n(a, #0:Fresh))),
   +(a ; b ; exp(g, n(a, #0:Fresh))), nil]  &
:: nil ::
[ nil |
   -(a),
   -(#2:Name ; exp(g, n(b, #3:Fresh))),
   +(a ; #2:Name ; exp(g, n(b, #3:Fresh))), nil]  &
:: nil ::
[ nil |
   -(b),
   -(exp(g, n(a, #0:Fresh))),
   +(b ; exp(g, n(a, #0:Fresh))), nil]  &
:: nil ::
```

[9] Note that expressions such as `irr(X:Msg)` or `inst(X:Msg)` included into the intruder knowledge require that message `X:Msg` has to be strongly irreducible (see definition in Page 16). The difference between `irr` and `inst` is that `inst` considers only new variables introduced by instantiation whereas `irr` any term in general. These constraints are dynamically checked, in order to discard states not satisfying them.

```
[ nil |
   -(#2:Name),
   -(exp(g, n(b, #3:Fresh))),
   +(#2:Name ; exp(g, n(b, #3:Fresh))), nil]  &
:: nil ::
[ nil |
   -(a ; b ; exp(g, n(b, #3:Fresh))),
   +(b ; exp(g, n(b, #3:Fresh))), nil]  &
:: nil ::
[ nil |
   -(a ; #2:Name ; exp(g, n(a, #0:Fresh))),
   +(#2:Name ; exp(g, n(a, #0:Fresh))), nil]  &
:: nil ::
[ nil |
   -(b ; exp(g, n(b, #3:Fresh))),
   +(exp(g, n(b, #3:Fresh))), nil]  &
:: nil ::
[ nil |
   -(#2:Name ; exp(g, n(a, #0:Fresh))),
   +(exp(g, n(a, #0:Fresh))), nil]  &
:: #3:Fresh ::
[ nil |
   -(a ; b ; exp(g, n(a, #0:Fresh))),
   +(a ; b ; exp(g, n(b, #3:Fresh))),
   -(e(exp(g, n(a, #0:Fresh) <+> n(b, #3:Fresh)), sec(a, #1:Fresh))), nil]  &
:: #0:Fresh,#1:Fresh ::
[ nil |
   +(a ; #2:Name ; exp(g, n(a, #0:Fresh))),
   -(a ; #2:Name ; exp(g, n(b, #3:Fresh))),
   +(e(exp(g, n(a, #0:Fresh) <+> n(b, #3:Fresh)), sec(a, #1:Fresh))), nil] )
||
e(exp(g, n(a, #0:Fresh) <+> n(b, #3:Fresh)), sec(a, #1:Fresh)) !inI,
exp(g, n(a, #0:Fresh)) !inI,
exp(g, n(b, #3:Fresh)) !inI,
(a ; b ; exp(g, n(a, #0:Fresh))) !inI,
(a ; b ; exp(g, n(b, #3:Fresh))) !inI,
(a ; #2:Name ; exp(g, n(a, #0:Fresh))) !inI,
(a ; #2:Name ; exp(g, n(b, #3:Fresh))) !inI,
(b ; exp(g, n(a, #0:Fresh))) !inI,
(b ; exp(g, n(b, #3:Fresh))) !inI,
(#2:Name ; exp(g, n(a, #0:Fresh))) !inI,
(#2:Name ; exp(g, n(b, #3:Fresh))) !inI
||
+(a ; #2:Name ; exp(g, n(a, #0:Fresh))),
-(a ; #2:Name ; exp(g, n(a, #0:Fresh))),
+(#2:Name ; exp(g, n(a, #0:Fresh))),
-(#2:Name ; exp(g, n(a, #0:Fresh))),
+(exp(g, n(a, #0:Fresh))),
-(b),
-(exp(g, n(a, #0:Fresh))),
+(b ; exp(g, n(a, #0:Fresh))),
-(a),
-(b ; exp(g, n(a, #0:Fresh))),
+(a ; b ; exp(g, n(a, #0:Fresh))),
-(a ; b ; exp(g, n(a, #0:Fresh))),
+(a ; b ; exp(g, n(b, #3:Fresh))),
-(a ; b ; exp(g, n(b, #3:Fresh))),
+(b ; exp(g, n(b, #3:Fresh))),
-(b ; exp(g, n(b, #3:Fresh))),
+(exp(g, n(b, #3:Fresh))),
-(#2:Name),
-(exp(g, n(b, #3:Fresh))),
+(#2:Name ; exp(g, n(b, #3:Fresh))),
-(a),
-(#2:Name ; exp(g, n(b, #3:Fresh))),
+(a ; #2:Name ; exp(g, n(b, #3:Fresh))),
-(a ; #2:Name ; exp(g, n(b, #3:Fresh))),
+(e(exp(g, n(a, #0:Fresh) <+> n(b, #3:Fresh)), sec(a, #1:Fresh))),
-(e(exp(g, n(a, #0:Fresh) <+> n(b, #3:Fresh)), sec(a, #1:Fresh)))
||
nil
|| never((#4:StrandSet &
:: #5:FreshSet ::
[ nil |
   +(a ; b ; exp(g, n(a, #0:Fresh))),
   -(a ; b ; exp(g, n(b, #3:Fresh))),
   +(e(#6:Exp, sec(a, #1:Fresh))), nil] ) || #7:IntruderKnowledge))
```

We note, however, that this is *not* the famous man-in-the-middle attack on unauthenticated Diffie-Hellman. Instead, it is a much more trivial attack in which the attacker removes the appended names from the initiator's message and substitutes some others. Thus, the responder is sharing a key with an honest initiator, just not the initiator he thinks. Furthermore, the other attack that Maude-NPA displays is only a slight variant.

The reason Maude-NPA finds the trivial attack and not the man-in-the-middle attack is because of the way Maude-NPA optimizes its search (see Appendix D). If it finds two states S_1 and S_2 such that the unreachability of S_1 implies the unreachability of S_2 it discards S_2 and keeps S_1. If S_1 leads to an attack, then it could be S_2 would have led to a different attack. In other words, if a protocol is insecure, Maude-NPA will find at least one attack, but it is not guaranteed to find all attacks possible.

Let's try asking Maude-NPA a different question. An intruder may not only want to mislead principals about who they are talking to, but to find out the secret himself. So we ask the following question:

```
eq ATTACK-STATE(1)
 = :: r ::
   [nil, -(a ; b ; XE),
         +(a ; b ; exp(g,n(b,r))),
         -(e(exp(XE,n(b,r)),sec(a,r'))) | nil]
   || sec(a,r') inI
   || nil
   || nil
   || nil
[nonexec] .
```

and we get the Man-in-the-Middle attack as follows[10]:

```
< (1[2]) . 5 . 3 . 17 . (0{1}) . 2 . 13 . 12 . 11 . 11 . 11 . 1 . 6 . 1 > (
:: nil ::
```

[10] The keyword `resuscitated` in the actual message list exchanged by the principals is included only for debugging purposes and does not imply any exchange between principals.

```
[ nil |
   -(exp(g, n(a, #3:Fresh))),
   -(#4:NeNonceSet),
   +(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh))), nil]  &
:: nil ::
[ nil |
   -(exp(g, n(b, #0:Fresh))),
   -(#1:NeNonceSet),
   +(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh))), nil]  &
:: nil ::
[ nil |
   -(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh))),
   -(sec(a, #2:Fresh)),
   +(e(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh)), sec(a, #2:Fresh))), nil]  &
:: nil ::
[ nil |
   -(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh))),
   -(e(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh)), sec(a, #2:Fresh))),
   +(sec(a, #2:Fresh)), nil]  &
:: nil ::
[ nil |
   -(a ; b ; exp(g, n(b, #0:Fresh))),
   +(b ; exp(g, n(b, #0:Fresh))), nil]  &
:: nil ::
[ nil |
   -(a ; #5:Name ; exp(g, n(a, #3:Fresh))),
   +(#5:Name ; exp(g, n(a, #3:Fresh))), nil]  &
:: nil ::
[ nil |
   -(b ; exp(g, n(b, #0:Fresh))),
   +(exp(g, n(b, #0:Fresh))), nil]  &
:: nil ::
[ nil |
   -(#5:Name ; exp(g, n(a, #3:Fresh))),
   +(exp(g, n(a, #3:Fresh))), nil]  &
:: #0:Fresh ::
[ nil |
   -(a ; b ; exp(g, #1:NeNonceSet)),
   +(a ; b ; exp(g, n(b, #0:Fresh))),
   -(e(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh)), sec(a, #2:Fresh))), nil]  &
:: #2:Fresh,#3:Fresh ::
[ nil |
   +(a ; #5:Name ; exp(g, n(a, #3:Fresh))),
   -(a ; #5:Name ; exp(g, #4:NeNonceSet)),
   +(e(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh)), sec(a, #2:Fresh))), nil] )
||
#1:NeNonceSet !inI,
#4:NeNonceSet !inI,
sec(a, #2:Fresh) !inI,
e(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh)), sec(a, #2:Fresh)) !inI,
e(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh)), sec(a, #2:Fresh)) !inI,
exp(g, n(a, #3:Fresh)) !inI,
exp(g, n(b, #0:Fresh)) !inI,
exp(g, #1:NeNonceSet <+> n(b, #0:Fresh)) !inI,
exp(g, #4:NeNonceSet <+> n(a, #3:Fresh)) !inI,
(a ; b ; exp(g, #1:NeNonceSet)) !inI,
(a ; b ; exp(g, n(b, #0:Fresh))) !inI,
(a ; #5:Name ; exp(g, #4:NeNonceSet)) !inI,
(a ; #5:Name ; exp(g, n(a, #3:Fresh))) !inI,
(b ; exp(g, n(b, #0:Fresh))) !inI,
(#5:Name ; exp(g, n(a, #3:Fresh))) !inI,
inst(#1:NeNonceSet),
exp(g, #1:NeNonceSet <+> n(b, #0:Fresh)) != exp(g, #4:NeNonceSet <+> n(a, #3:Fresh))
||
generatedByIntruder(#1:NeNonceSet),
generatedByIntruder(a ; b ; exp(g, #1:NeNonceSet)),
-(a ; b ; exp(g, #1:NeNonceSet)),
+(a ; b ; exp(g, n(b, #0:Fresh))),
-(a ; b ; exp(g, n(b, #0:Fresh))),
+(b ; exp(g, n(b, #0:Fresh))),
generatedByIntruder(a ; #5:Name ; exp(g, #4:NeNonceSet)),
+(a ; #5:Name ; exp(g, n(a, #3:Fresh))),
-(a ; #5:Name ; exp(g, n(a, #3:Fresh))),
+(#5:Name ; exp(g, n(a, #3:Fresh))),
-(b ; exp(g, n(b, #0:Fresh))),
+(exp(g, n(b, #0:Fresh))),
-(#5:Name ; exp(g, n(a, #3:Fresh))),
+(exp(g, n(a, #3:Fresh))),
-(exp(g, n(b, #0:Fresh))),
-(#1:NeNonceSet),
+(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh))),
generatedByIntruder(#4:NeNonceSet),
-(exp(g, n(a, #3:Fresh))),
-(#4:NeNonceSet),
+(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh))),
-(a ; #5:Name ; exp(g, #4:NeNonceSet)),
+(e(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh)), sec(a, #2:Fresh))),
resuscitated(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh))),
-(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh))),
-(e(exp(g, #4:NeNonceSet <+> n(a, #3:Fresh)), sec(a, #2:Fresh))),
+(sec(a, #2:Fresh)),
-(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh))),
-(sec(a, #2:Fresh)),
+(e(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh)), sec(a, #2:Fresh))),
-(e(exp(g, #1:NeNonceSet <+> n(b, #0:Fresh)), sec(a, #2:Fresh)))
||
nil
||
nil
```

The lesson to be learned here is that one must be sure to query Maude-NPA about *all* the properties that a protocol is supposed to have before concluding that it is secure.

6 Protocol Search with Never Patterns

The search space generated by Maude-NPA can be very large, and it is convenient to use never patterns in the attack state to restrict the search space, as well as to define that attack state. Let us consider the Diffie-Hellman protocol (Section 5.3 with some never patterns in order to reduce the search space. Consider the following attack state with never patterns.

```
eq ATTACK-STATE(2)
 = :: r ::
   [nil, -(a ; b ; XE),
         +(a ; b ; exp(g,n(b,r))),
         -(e(exp(XE,n(b,r)),sec(a,r'))) | nil]
```

```
     || sec(a,r') inI
     || nil
     || nil
     || never(
     *** Avoid infinite useless path
      (:: nil ::
      [ nil | -(exp(GE,NS1 * NS2)), -(NS3),
          +(exp(GE,NS1 * NS2 * NS3)), nil ]
      & S:StrandSet || K:IntruderKnowledge)
     *** Pattern to avoid unreachable states
     (:: nil ::
      [nil | -(exp(#1:Exp, N1:Nonce)),
             -(sec(A:Name, #2:Fresh)),
             +(e(exp(#1:Exp, N2:Nonce), sec(A:Name, #2:Fresh))), nil]
      & S:StrandSet || K:IntruderKnowledge)
     *** Pattern to avoid unreachable states
     (:: nil ::
      [nil | -(exp(#1:Exp, N1:Nonce)),
          -(e(exp(#1:Exp, N1:Nonce), S:Secret)),
          +(S:Secret), nil]
      & S:StrandSet || K:IntruderKnowledge)
     *** Pattern to avoid unreachable states
     (S:StrandSet
      || (#4:Gen != #0:Gen), K:IntruderKnowledge)
     )
  [nonexec] .
```

Let us explain the never patterns used above. There are two kinds of never patterns: (1) concrete intruder actions that lead to infinite search patterns (in some protocols this may generate an infinite search space and its removal by a never pattern may provide a finite search space) and (2) unreachable states that appear in the search space, that will ultimately be shown unreachable but nevertheless increase its size. We note, however, that the use of the first type of never pattern can mean that failure to find an attack no longer guarantees security. It is most useful when testing new equational theories whose behavior is not that well understood yet. We describe each of these never patterns in detail below:

- The intruder strand

  ```
  [ nil | -(exp(GE,NS1 * NS2)), -(NS3),
       +(exp(GE,NS1 * NS2 * NS3)), nil ]
  ```

  leads to a bigger search space involving larger and larger nonce sets. Since the protocol requires only a nonce set of size two to execute, it appears safe as a first approximation to exclude any intruder strands that create a nonce set of size three or more.

- The intruder strand

```
[nil | -(exp(#1:Exp, N1:Nonce)), -(sec(A:Name, #2:Fresh)),
       +(e(exp(#1:Exp, N2:Nonce), sec(A:Name, #2:Fresh))), nil]
```

is unreachable, since there is no way that the negative term `exp(#1:Exp,Nonce)` can be irreducible, as required. [11]

- The intruder strand

  ```
  [nil | -(exp(#1:Exp, N1:Nonce)), -(e(exp(#1:Exp, N1:Nonce), S:Secret)),
         +(S:Secret), nil]
  ```

  is unreachable, for the same reason.

- Any generated state containing the constraint `#4:Gen != #0:Gen` is unreachable, since there is only one term of sort `Gen`, namely constant `g`.

We try running this attack state with never patterns, and compare it with the output of the same attack state with never patterns:

Attack State	1	2	3	4	5	6	7	8	9	10	11	12
w/o nevers	4	6	11	10	15	16	23	17	6	3	2	1
with nevers	3	4	5	5	7	6	6	5	4	3	2	1

Although never patterns can have a dramatic effect on search space size, they should be used with care, because improper use of never patterns can cause Maude-NPA to miss a genuine attack. However, using never patterns to reduce search space size can be very useful in debugging protocols, since they allow the user to pinpoint weaknesses without performing a full-scale Maude-NPA search.

One important technique used in both the NRL-Protocol Analyzer and the Maude-NPA is the use of *grammars* [26, 12] to characterize sets of *unreachable* states, that is, states from which, through backwards search, it is provably impossible to reach an initial state (see Section 3.4). Grammars can drastically cut down the search space and often allow backwards search to terminate in many cases where unrestricted search would not. Appendix B gives a more detailed description of grammars in the Maude-NPA.

If nothing is specified by the user in a protocol specification, the Maude-NPA automatically generates grammars for such a protocol in a way entirely transparent to the user. However, to further constrain the search space without losing completeness, it is possible for the user to suggest additional grammars, as "initial grammars", that are both tested and completed by the Maude-NPA into "final grammars" where all the generated terms are provably unreachable.

A good case in point is the present Diffie-Hellman example, where one such initial grammars is indeed useful in further constraining the attack search. We do not give the grammar here, but instead refer to Appendix B.2, where such a grammar is presented and explained, and to Appendix F.5, where the full protocol specification

[11] Recall that received messages (negative terms) are always supposed to be in irreducible form.

for the Diffie-Hellman example, including the specification of the above-mentioned initial grammar, is given.

Besides grammars, the Maude-NPA uses a variety of other state-space reduction techniques. When used in combination with grammars, these can drastically cut down the search space size. Indeed, in a good number of cases these techniques reduce what would be an infinite number of states to a *finite* number, so that termination of the Maude-NPA without finding an attack provides *full verification* that the attack searched for is impossible under the assumptions of the specification. The state space reduction techniques are intended to be transparent to the user, so we do not discuss them in the main body of the manual and refer the reader to [17]. However, for the sake of documentation, we include a brief discussion of them, with references, in Appendix D.

7 Known Limitations and Future Work

In this section we describe some known limitations, along with the work we plan to do in the future to address them. Where workarounds exist, we also describe those.

1. In some cases, the automatic grammar generation fails to terminate, although these cases are rare. At this point, the only way of addressing this problem is to specify the initial grammars oneself, instead of having the tool generate them. How this is done is explained in Appendix B. In practice, sometimes the process fails to terminate because some Dolev-Yao strands are missing in the specification.

2. In other cases, although the grammar generation terminates, it takes a long time, and it is tedious to recompute every time a specification is loaded. One can save the grammars by first reducing the `genGrammars` command in Maude, and copying and pasting the results to the specification. How this is done is described in Appendix B.

3. The unification algorithm of a user-defined equational theory does not terminate for arbitrary equational theories. For a detailed description of the theories of interest for which it does and does not terminate, and our plans to extend the current class of supported theories to theories satisfying the finite variant property, see Section 3.2.6 and Appendix A.

4. In some cases, when a unification algorithm would produce an infinite number of unifiers, it is possible to obtain a *finitary* unification algorithm by a judicious use of sorts. For more details on this, see Appendix A and [13] for bounded associativity.

5. In some finitary cases, the number of unifiers produced, although finite, is so large that it crashes Maude-NPA. This is currently happening for many protocols using exclusive-or, for example. In many cases, these unifiers are redundant.

References

[1] María Alpuente, Santiago Escobar, and José Iborra. Termination of narrowing revisited. *Theoretical Computer Science*, 410(46):4608–4625, 2009.

[2] Siva Anantharaman, Hai Lin, Christopher Lynch, Paliath Narendran, and Michaël Rusinowitch. Cap unification: application to protocol security modulo homomorphic encryption. In *ASIACCS*, pages 192–203. ACM, 2010.

[3] Siva Anantharaman, Paliath Narendran, and Michaël Rusinowitch. Unification modulo *cui* plus distributivity axioms. *Journal of Automated Reasoning*, 33(1):1–28, 2004.

[4] Franz Baader and Klaus U. Schulz. Unification in the union of disjoint equational theories: Combining decision procedures. In *CADE*, volume 607 of *LNCS*, pages 50–65. Springer, 1992.

[5] M. Clavel, F. Durán, S. Eker, J. Meseguer, P. Lincoln, N. Martí-Oliet, and C. Talcott. *All About Maude – A High-Performance Logical Framework.* Springer LNCS Vol. 4350, 2007.

[6] Hubert Comon-Lundh and Stéphanie Delaune. The finite variant property: How to get rid of some algebraic properties. In Jürgen Giesl, editor, *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2005.

[7] Hubert Comon-Lundh and Stéphanie Delaune. The finite variant property: How to get rid of some algebraic properties. In *RTA*, pages 294–307, 2005.

[8] Nachum Dershowitz, Subrata Mitra, and G. Sivakumar. Decidable matching for convergent systems (preliminary version). In Deepak Kapur, editor, *11th International Conference on Automated Deduction (CADE-11)*, volume 607 of *Lecture Notes in Computer Science*, pages 589–602. Springer, 1992.

[9] Francisco Durán, Steven Eker, Santiago Escobar, José Meseguer, and Carolyn L. Talcott. Variants, unification, narrowing, and symbolic reachability in maude 2.6. In Manfred Schmidt-Schauß, editor, *Proceedings of the 22nd International Conference on Rewriting Techniques and Applications, RTA 2011, May 30 - June 1, 2011, Novi Sad, Serbia*, volume 10 of *LIPIcs*, pages 31–40. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2011.

[10] S. Escobar, J. Hendrix, C. Meadows, and J. Meseguer. Diffie-Hellman cryptographic reasoning in the Maude-NRL protocol analyzer. In *Proc. 2nd International Workshop on Security and Rewriting Techniques (SecReT 2007)*, 2007.

[11] S. Escobar, D. Kapur, C. Lynch, C. Meadows, J. Meseguer, P. Narendran, and R. Sasse. Protocol analysis in Maude-NPA using unification modulo homomorphic encryption. In Michael Hanus, editor, *13th International ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP 2011)*. ACM Press, 2011.

[12] S. Escobar, C. Meadows, and J. Meseguer. A rewriting-based inference system for the NRL protocol analyzer and its meta-logical properties. *Theoretical Compute Science*, 367(1–2):162–202, 2006.

[13] S. Escobar, C. Meadows, and J. Meseguer. Equational cryptographic reasoning in the Maude-NRL protocol analyzer. In *Proc. 1st International Workshop on Security and Rewriting Techniques (SecReT 2006)*, pages 23–36. ENTCS 171(4) , Elsevier, 2007.

[14] S. Escobar, J. Meseguer, and R. Sasse. Variant narrowing and equational unification. Technical Report UIUCDCS-R-2007-2910, Dept. of Computer Science, University of Illinois at Urbana-Champaign, October 2007.

[15] Santiago Escobar, Catherine Meadows, and José Meseguer. State space reduction in the maude-nrl protocol analyzer. In Sushil Jajodia and Javier López, editors, *Computer Security - ESORICS 2008, 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings*, volume 5283 of *Lecture Notes in Computer Science*, pages 548–562. Springer, 2008.

[16] Santiago Escobar, Catherine Meadows, and José Meseguer. Maude-NPA: Cryptographic protocol analysis modulo equational properties. In *Foundations of Security Analysis and Design V, FOSAD 2007/2008/2009 Tutorial Lectures*, LNCS vol. 5705, pages 1–50. Springer, 2009.

[17] Santiago Escobar, Catherine Meadows, and José Meseguer. State space reduction in the maude-nrl protocol analyzer. *CoRR*, abs/1105.5282, 2011.

[18] Santiago Escobar, José Meseguer, and Ralf Sasse. Effectively checking the finite variant property. In Andrei Voronkov, editor, *Rewriting Techniques and Applications, 19th International Conference, RTA 2008, Hagenberg, Austria, July 15-17, 2008, Proceedings*, volume 5117 of *Lecture Notes in Computer Science*, pages 79–93. Springer, 2008.

[19] Santiago Escobar, Ralf Sasse, and José Meseguer. Folding variant narrowing and optimal variant termination. *J. Log. Algebr. Program.*, 2010. In Press.

[20] F. J. Thayer Fabrega, J. Herzog, and J. Guttman. Strand Spaces: What Makes a Security Protocol Correct? *Journal of Computer Security*, 7:191–230, 1999.

[21] Joe Hendrix and José Meseguer. Order-sorted equational unification revisited. *Electr. Notes Theor. Comput. Sci.*, 2008. To appear in Proc. of RULE 2008.

[22] Jean-Marie Hullot. Canonical forms and unification. In Wolfgang Bibel and Robert Kowalski, editors, *Proceedings, Fifth Conference on Automated Deduction*, pages 318–334. Springer-Verlag, 1980. LNCS, Volume 87.

[23] J.-P. Jouannaud, C. Kirchner, and H. Kirchner. Incremental construction of unification algorithms in equational theories. In *Proc. ICALP'83*, pages 361–373. Springer LNCS 154, 1983.

[24] Christopher Lynch and Catherine Meadows. On the relative soundness of the free algebra model for public key encryption. In *Workshop on Issues in Theory of Security 2004*, 2004.

[25] Christopher Lynch and Catherine Meadows. Sound approximations to Diffie-Hellman using rewrite rules. In *Proceedings of the International Conference on Information and Computer Security (ICICS)*. Springer-Verlag, 2004.

[26] Catherine Meadows. Language generation and verification in the NRL protocol analyzer. In *Ninth IEEE Computer Security Foundations Workshop, March 10 - 12, 1996, Dromquinna Manor, Kenmare, County Kerry, Ireland*, pages 48–61. IEEE Computer Society, 1996.

[27] Jonathan Millen. On the freedom of decryption. *Information Processing Letters*, 86(3), 2003.

[28] Ralf Sasse, Santiago Escobar, Jose Meseguer, and Catherine Meadows. Protocol analysis modulo combination of theories: A case study in Maude-NPA. In *6th International Workshop on Security and Trust Management (STM'2010), Revised Selected Papers*. Springer, 2010.

[29] Stuart Stubblebine and Catherine Meadows. Formal characterization and automated analysis of known-pair and chosen-text attacks. *IEEE Journal on Selected Areas in Communications*, 18(4):571–581, 2000.

[30] Emanuele Viola. E-unifiability via narrowing. In Antonio Restivo, Simona Ronchi Della Rocca, and Luca Roversi, editors, *Theoretical Computer Science, 7th Italian Conference, ICTCS 2001, Torino, Italy, October 4-6, 2001, Proceedings*, volume 2202 of *Lecture Notes in Computer Science*, pages 426–438. Springer, 2001.

A Narrowing-based Finitary Equational Unification

In the standard Dolev-Yao model, symbolic reachability analysis typically takes the form of representing sets of states symbolically as terms with logical variables, and then performing *syntactic unification* with the protocol rules to explore reachable states. This can be done in either a forwards or a backwards fashion. In the Maude-NPA (which can also be used for analyses under the standard Dolev-Yao model when no algebraic properties are specified) symbolic reachability analysis is performed in a *backwards* fashion, beginning with a symbolic representation of an attack state, and searching for an initial state, which then provides a proof that an attack is possible; or a proof that no such attack is possible if all such search paths fail to reach an initial state.

However, if the Maude-NPA analyzes a protocol for which algebraic properties *have* been specified by an equational theory T, the same symbolic reachability analysis is performed in the same fashion, but now *modulo* T. What this means precisely is that, instead of performing syntactic unification between a term representing symbolically a set of states and the righthand-side (in the backwards reachability case) of a protocol rule, we now perform *equational unification* with the theory T, (also called T-*unification*, or *unification modulo* T) between the same term and the same righthand side of a protocol rule. The following sections explain several things regarding T-unification in the Maude-NPA:

- Equational axioms for which the Maude-NPA provides built-in support for equational unification.
- Narrowing-based equational unification in general, which is however infeasible for Maude-NPA analysis when the number of unifiers generated is infinite; and
- The most general case of equational theories for which the Maude-NPA can currently support unification by narrowing, with the important requirement of the number of unifier solutions being *finite*, namely, the admissible theories described in Section 3.2.6.
- Specialized unification algorithms also provided for theories that cannot be handled by narrowing and that do not have built-in support in Maude.
- Integration of different unification algorithms.

A.1 Built-in support for Unification Modulo Equational Axioms

The Maude-NPA has built-in support for unification modulo certain equational theories T thanks to the underlying Maude infrastructure [9]. Specifically, the Maude-NPA automatically supports unification modulo T for T any order-sorted theory of the form $T = (\Sigma, Ax)$, where Ax is a collection of equational *axioms* where some binary operators f in the signature Σ may have axioms in Ax for either (i) *commutativity* ($f(x,y) = f(y,x)$), (ii) commutativity and *associativity* ($f(x,f(y,z)) = f(f(x,y),z)$), or (iii) commutativity, associativity and *identity element* e ($f(x,e) = x$). Associativity without commutativity is not supported, because it is well-known that unification problems modulo associativity may have an *infinite* number of unifiers. Commutativity with identity is also not supported but it is available through the narrowing-based unification algorithm of Section 3.2.6 and Appendix A.2. As already illustrated in Section 3.2.2, the way associativity, and/or commutativity, and/or identity axioms are specified in Maude for a function symbol f is not by giving those axioms explicitly, but by declaring f in Maude with the `assoc` and/or `comm` and/or `id:` attributes. For example a function symbol `f` of sort `S` which is associative, commutative, and with identity element `nil` is specified in Maude as follows:

```
op f : S S -> S [assoc comm id: nil] .
```

A.2 Narrowing-Based Equational Unification and its Limitations

Of course, many algebraic theories T of interest in protocol analysis fall outside the scope of the above-mentioned class of theories T based on combinations of associativity and/or commutativity and/or identity axioms, for which the Maude-NPA provides automatic built-in support. Therefore, the burning issue is how to support more general classes of algebraic theories in the Maude-NPA.

In this regard, a very useful, generic method to obtain T-unification algorithms is *narrowing* [22, 23]. In order for narrowing to provide a T-unification algorithm, the theory T has to be of the form $T = (\Sigma, E \cup Ax)$, where Ax is a collection of equational axioms such as our previous combinations of associativity and/or commutativity and/or identity axioms for which a *finitary* Ax-unification algorithm exists (that is, any Ax-unification problem has a finite number of unifiers providing a complete set of solutions), and E is a collection of equations that, as rewrite rules, are:

1. confluent modulo Ax
2. terminating modulo Ax, and
3. coherent modulo Ax (see [23]).

The precise meaning of these three requirements was explained in detail in Section 3.2.6.

Although narrowing is a very general method to generate T-unification algorithms, general narrowing has a serious limitation. The problem is that, in general, narrowing with an equational theory $T = (\Sigma, E \cup Ax)$ satisfying requirements (1)–(3) above yields an *infinite* number of unifiers. Since, for T the algebraic theory of a protocol, T-unification must be performed by the Maude-NPA at each *single step* of symbolic reachability analysis, narrowing is in general not practical as a unification procedure, unless the theory T satisfies the additional requirement that there always exists a *finite* set of unifiers that provide a complete set of solutions; and that such a finite set of solutions can be effectively computed by narrowing. We discuss this extra important requirement in what follows.

A.3 Narrowing-Based Equational Unification in the Maude-NPA

Sufficient conditions for narrowing-based T-unification to provide a finite, complete set of solutions are known. For example, for the case when $T = (\Sigma, E \cup Ax)$ and $Ax = \emptyset$ such sufficient conditions go back to [22, 8]; see [1] for a recent survey.

The case when $Ax \neq \emptyset$ is considerably more challenging (see, e.g., [6, 30, 14, 19]). However, the condition of *strong right irreducibility* in [14], applies to both cases ($Ax = \emptyset$ and $Ax \neq \emptyset$) and is easy to check. This condition was already explained in detail in Section 3.2.6 and ensures that there is always a finite number of unifiers modulo $E \cup Ax$.

As already mentioned in Sections 3.2.6 and 3.2.7, the Maude-NPA's support for order-sorted specifications is very helpful in achieving strong right irreducibility, and therefore in reaching the desired goal of obtaining a finite complete set of unifiers by narrowing. This is because unification problems that may have an infinite number of unifiers in an untyped setting can sometimes have only a finite set of unifiers in a setting with types and subtypes. The key reason is that many of the untyped unifiers do not even typecheck. In the Maude-NPA, order-sortedness can sometimes be directly used to one's advantage to obtain strongly right irreducible theories T that have finitary T-unification algorithms. Furthermore, order-sortedness can greatly help in having smaller search spaces for symbolic reachability, since many unifiers that would have to be explored in an untyped setting are weeded out by the inherent type checking of order-sorted unification.

A more general condition than strong right irreducibility, call the *finite variant property* has been recently proposed by Comon and Delaune [6]. This condition is satisfied by a number of useful cryptographic theories, even beyond theories with the strong right irreducibility condition. Furthermore, in [19] it is shown how a finitary unification algorithm can be obtained in these theories. Methods for checking the finite variant property are proposed in [18, 19]. In a future version of Maude-NPA we plan to support narrowing-based unification for the broader class of theories enjoying the finite variant property.

A.4 Unification for Homomorphic Encryption over Concatenation

Although the ease of implementation of narrowing-based unification makes it very useful for exploration and experimentation, and interesting cryptographic theories satisfy the finite variant property, ultimately we also want to be able to make use of more efficient special-purpose algorithms. Moreover, there is a class of equational theories that appears prominently in cryptographic protocols applied to privacy-preserving computation: operators that are homomorphic with respect to another, e.g., $q(X * Y) = q(X) * q(Y)$. Theories like these can be shown to lack the finite variant property whether or not $*$ is a free operator or obeys the axioms for an Abelian group.[12] In these cases narrowing-based unification does not provide a finitary E-unification algorithm, and we must seek a different method.

An algorithm for unification modulo the homomorphic encryption theory E_h defined by the single oriented equation $e(X;Y,Z) \to e(X,Z);e(Y,Z)$ in a signature containing symbols e, $\_;\_$, and uninterpreted function symbols was given in [2]. The inference rules given in [2] were proved to be sound, complete, and terminating

[12] Comon and Delaune only prove the result for the exclusive-or case in [7], but their proof can easily be extended to the other cases.

meaning that all solved forms created by the algorithm are correct solutions of the unification problem and that for every solution of the unification problem there is a more general solution created by the algorithm. This algorithm was implemented in Maude using the metalevel facilities, providing an algorithm parametric on the symbols e and $\_;\_$ chosen by the user. The implementation and its integration into Maude-NPA were described in [11].

The implemented algorithm was untyped and an order-sorted version of the unification algorithm was automatically derived following the methodology proposed in [21]. This methodology applies a general algorithm by which, under mild conditions on the theory E, an order-sorted E-unification algorithm can be automatically obtained by: (i) associating to E its unsorted version $\bar{E}$; (ii) computing a complete set of (unsorted) $\bar{E}$-unifiers for the given E-unification problem; and (iii) typing and filtering out the unsorted $\bar{E}$-unifiers to obtain a complete set of order-sorted E-unifiers using the generic *sort propagation algorithm* described in [21]. This algorithm has also been integrated into the Maude-NPA infrastructure but can also be applied in any other contexts in which one wants to derive an order-sorted unification algorithm from its unsorted version.

Finally, we combine E_h-unification with a typed version of ACU-unification. The latter is needed because Maude-NPA states are multisets of terms, which are associative-commutative and have the empty multiset as the identity. This combination is supported by Maude-NPA by means of an order-sorted variant of the standard combination method for disjoint theories à la Baader and Schultz [4], so that in the end typed $E_h \cup ACU$-unification is achieved. A more complete description of how this is done is given in [28].

A.5 Integration of Different Equational Unification Algorithms

Integrating equational unification into protocol analysis is challenging for several reasons. First of all, in principle we need to have a different $E_{\mathcal{P}}$-unification algorithm for each protocol $\mathcal{P}$; second, experience with the Maude-NPA tool has shown the great advantages (typically leading to a much smaller search space) of *typed unification*, where variables have types (or *sorts*) and types can be arranged in *subtype hierarchies*; for example, to properly specify a protocol we may wish to distinguish different subtypes —e.g., for nonces, keys, or principal names— of a general type for messages; third, we often need to *combine* several such unification algorithms, for example when composing together various subprotocols or taking into account the associative-commutative-identity (ACU) axioms of the state constructors (see Section 3). This is made even more challenging by the fact that, in order to allow the option of verifying different kinds of implementations (e.g. the case in which a key is indistinguishable from a nonce), typing is mostly left to the discretion of the user.

Given the wide range of protocols and protocol combinations that need to be analyzed, a *modular* approach to the development of $E_{\mathcal{P}}$-unification algorithms is very much needed. Such a modular approach and its necessary infrastructure are now under development. Besides using the known techniques for combining unification algorithms for disjoint theories à la Baader and Schultz [4], Maude-NPA employs a more general methodology and associated tool infrastructure (in the Maude-NPA) in which unification algorithms can be combined and developed at three different levels and in a not necessarily disjoint way: (i) a basic library of commonly occurring theories and their combinations —currently including any combination of typed commutative, associative commutative, associative commutative and identity, or free function symbols— is efficiently supported by the Maude tool at the C++ level; (ii) unification algorithms for special-purpose cryptographic theories can be developed in a declarative way in Maude itself using its metalevel facilities as done in Section A.4 for the homomorphic encryption theory E_h; and (iii) it is often possible to decompose an equational theory $E_{\mathcal{P}}$ as a disjoint union $E_{\mathcal{P}} = \Delta \cup Ax$, (where Δ and Ax may share some function symbols), and where a dedicated Ax-unification algorithm exists. If Δ is viewed as a set of rewrite rules that is convergent, coherent and has the finite variant property modulo Ax, *folding variant narrowing modulo* Ax with the rules Δ provides a finitary $E_{\mathcal{P}}$-unification algorithm [19].

B Specifying Grammars

Grammars are used in Maude-NPA to eliminate various infinite search paths that can be provably guaranteed to never reach an initial state [12]. By an *initial grammar* we mean a grammar conjecturing a set of unreachable states. The conjecture of an initial grammar does not have to be correct and is just an initial guess. Instead, a *final grammar* is a grammar that has been checked by the Maude-NPA to correctly generate a set of states whose elements are all unreachable. Final grammars are generated iteratively by the Maude-NPA from initial grammars. The default in Maude-NPA is to generate both the initial and final grammars *completely automatically*, at the beginning of the first attack search after a specification is loaded (see Section 4 for a description of how to perform attack searches). The intent is for grammars to be completely transparent to the user. However, there are cases in which the user may want to reuse grammars, add initial grammars, or replace the initial grammars generated by the Maude-NPA with his or her own ones. We describe how to do all this below. We also describe the user-defined initial grammar used to cut down the search space of the attach search of the Diffie-Hellman protocol discussed in Section 5.3.

B.1 Reusing Grammars

The generation of grammars may be time-consuming, and the user may want to avoid having to do this every time a specification is reloaded. This can be avoided by adding the grammars to the specification. One first displays the grammars by reducing the `genGrammars` constant in Maude-NPA typing:

```
red genGrammars .
```

Maude-NPA will then produce output of the form

```
result GrammarList:

... Grammars ...
```

To reuse the grammars displayed by Maude-NPA in this way in a subsequent execution of the protocol, the user should "cut and paste" these grammars in an equation of the form:

```
eq GENERATED-GRAMMARS =

... Grammars ...

[nonexec] .
```

where `...Grammars..` is the text that was generated by the `genGrammars` command. Note that the `genGrammars` command can fail to generate a grammar for a concrete initial grammar. Such failure grammars are identified by terms starting with `errorNoHeuristicApplied`, `errorIntegratingExceptions`, and `errorInconsistentExceptionsInGrammarRule`. Failure grammars cannot be included in the `GENERATED-GRAMMARS` equation. The `GENERATED-GRAMMARS` equation is added to the module `PROTOCOL-SPECIFICATION` in the general template described in Section 3, right before the attack state specifications. Maude-NPA will now treat these as the initial grammars.

B.2 Adding New Initial Grammars

There are still some cases in which the initial grammars generated by Maude-NPA are not sufficient. In such a case the user can add his or her own initial grammars. For example, the Diffie-Hellmman protocol specified in Section 5.3 requires the following initial grammar, which is not yet automatically generated by Maude-NPA:

```
    grl empty => (NS * n(a,r)) inL . ;
    grl empty => n(a,r) inL . ;
    grl empty => (NS * n(b,r)) inL . ;
    grl empty => n(b,r) inL .
```

This initial grammar indicates that the concrete nonces generated by the initiator and the responder cannot be learned by the intruder, independently of whether they are combined with other nonces.

This can be done by adding an `EXTRA-GRAMMARS` equation to the `PROTOCOL-SPECIFICATION` module of the three-module template and specifying the initial grammars there as the value of `EXTRA-GRAMMARS`, as in the following:

```
eq EXTRA-GRAMMARS
  = (grl empty => (NS * n(a,r)) inL . ;
     grl empty => n(a,r) inL . ;
     grl empty => (NS * n(b,r)) inL . ;
     grl empty => n(b,r) inL .
     ! S2 )
  [nonexec] .
```

Originally, initial grammars consisted of the definition of a single term (called the *seed-term*) but, as we see from the example above, an initial grammar can now be any syntactically correct grammar. Giving a complete set of directives on writing grammars is beyond the scope of this document, but we give a BNF specification of grammars in Appendix C. Strategies `S1` or `S2` for grammar generation are chosen depending on the conditions (`empty` requires strategy `S2` whereas (`Msg notInI` requires strategy `S1`). If the user wants to see what the initial grammars generated by Maude-NPA look like, this is done by reducing the expression `genGrammars(0)` in Maude (i.e., typing "`red genGrammars(0) .`"), where `0` indicates the number of grammar generation steps allowed and `unbounded` is the constant used in regular grammar generations.

We note that `GENERATED-GRAMMARS` has precedence over `EXTRA-GRAMMARS`. If both are found in a specification, `GENERATED-GRAMMARS` will be used and `EXTRA-GRAMMARS` will be ignored.

B.3 Replacing Maude-NPA Initial Grammars

In some cases one may want to replace the Maude-NPA initial grammars entirely. In this case, one uses `INITIAL-GRAMMARS` but enters one's own grammar specifications, following Appendix C, instead of the ones generated by Maude-NPA. This feature is only recommended for debugging Maude-NPA.

C Grammar BNF Syntax

In this Appendix we give a BNF specification of the syntax of Maude-NPA grammars. For a more complete discussion of grammars and how they work, see [12].

```
GrammarSpecList -> GrammarSpec | GrammarSpec "|" GrammarSpecList
GrammarSpec -> "(" Grammar "!" Strategy ")"
Strategy -> "S1" | "S2"
Grammar -> GrammarRule | GrammarRule ";" Grammar
GrammarRule _-> "grl" Conditions "=>" Term "inL ."
Conditions -> "empty" | Condition | Condition "," Conditions
Condition -> Term "notInI" | Term "inL" | Term "notLeq" Term
```

We do not provide a BNF definition of the production `Term`; that is just any term of sort `Msg` specifiable in the user-defined protocol syntax.

D Other Optimizations

In this section we describe the various optimization techniques, besides grammars, that the Maude-NPA uses to reduce the size of the search space. All of these are described in detail in [15, 17].

1. Partial Order Reduction. One of the possible backwards steps in a Maude-NPA analysis involves moving a negative strand into the intruder knowledge. If any of these steps are possible, they are always executed first.

2. Detecting Inconsistent States Early

   Certain types of states containing inconsistent information are eliminated early.

   a) A state St containing two contradictory facts (t `inI`) and (t `!inI`) for a term t.
   b) A state St whose intruder knowledge contains the fact (t `!inI`) and a strand of the form $[m_1^\pm, \ldots, t^-, \ldots, m_{j-1}^\pm \mid m_j^\pm, \ldots, m_k^\pm]$.
   c) A state St containing a fact (t `inI`) such that t contains a fresh variable r and the strand in St indexed by r, i.e., $(r_1, \ldots, r, \ldots, r_k : \mathsf{Fresh})$ $[m_1^\pm, \ldots, m_{j-1}^\pm \mid m_j^\pm, \ldots, m_k^\pm]$, cannot produce r, i.e., r is not a subterm of any output message in $m_1^\pm, \ldots, m_{j-1}^\pm$.
   d) A state St containing a strand of the form $[m_1^\pm, \ldots, t^-, \ldots, m_{j-1}^\pm \mid m_j^\pm, \ldots, m_k^\pm]$ for some term t such that t contains a fresh variable r and the strand in St indexed by r cannot produce r.

3. Transition Subsumption

   There are a number of cases in which it is possible to tell that a state S_1 is reachable only if another state S_2 is. Roughly speaking, this occurs when S_1 subsumes a substate of S_2. In that case, S_2 is deleted and only S_1 is kept. Whenever a new state is found, this transition subsumption check is done on it with all existing states, including states appearing higher up in the search tree, to determine whether or not it should be kept.

4. Super Lazy Intruder

   If variable terms, publicly known constants (such as names), or terms constructed out of variables and publicly known constants appear in the intruder knowledge, then there is no need to search for them, since it is trivial for the intruder to produce them. However, it is possible that later on in the search they may become instantiated, and it will then be necessary to reintroduce them. The solution is to remove these terms (called *super-lazy terms*) but keep the state in which they appear around as a *ghost state* which can be resuscitated if the variables in the terms are instantiated. The ghost states are stored in the fourth argument of the attack state in the backwards search.

E Commands Useful for Debugging

The following commands are mainly useful for debugging Maude-NPA; we include them for the sake of completeness.

E.1 Excluding Optimizations and Checks

For debugging purposes, it is possible to disable optimization techniques and validity checks on the data selectively. One adds another argument to the run or summary command, which includes the optimization techniques to be disabled. For example, if one wants to disable grammars and the inconsistency optimization techniques (the latter marks as unreachable states that violate certain consistency properties while looking for the second state in a backwards search), this is given as follows:

```
red run(0,2,-grammars -inconsistency) .
```

The optimization techniques that can be turned off are the following

1. `-grammars` turns off the grammars.
2. `-inconsistency` turns off inconsistency check 2.a described above
3. `-inputAndNotLearned` turns off inconsistency check 2.b
4. `-alreadySent` turns off inconsistency check 2.c
5. `-secretData` turns off inconsistency check 2.d
6. `-implication` turns off the transition subsumption
7. `-equationalRed` turns off the check that negative terms are irreducible
8. `-freshInstantiated`, turns off the check that fresh variables are never instantiated
9. `-inputFirst` turns off the partial order reduction 1.a
10. `-ghost` turns off the super-lazy intruder.
11. `-never` turns off the never patterns appearing in attack states.
12. `none` turns off all of the optimizations. Note that `-` is not used here.

F Example Protocol files

This appendix contains the full protocol specifications for the protocol examples used in this manual.

F.1 Needham-Schroeder Public Key Protocol

The contents of the file describing this protocol are as follows:

```
fmod PROTOCOL-EXAMPLE-SYMBOLS is
  --- Importing sorts Msg, Fresh, Public, and GhostData
  protecting DEFINITION-PROTOCOL-RULES .

  ----------------------------------------------------------
  --- Overwrite this module with the syntax of your protocol
  --- Notes:
  --- * Sort Msg and Fresh are special and imported
  --- * Sorts must be subsorts of Msg
  --- * No sort can be a supersort of Msg
  ----------------------------------------------------------

  --- Sort Information
  sorts Name Nonce Key .
  subsort Name Nonce Key < Msg .
  subsort Name < Key .
  subsort Name < Public .

  --- Encoding operators for public/private encryption
  op pk : Key Msg -> Msg [frozen] .
  op sk : Key Msg -> Msg [frozen] .

  --- Nonce operator
  op n : Name Fresh -> Nonce [frozen] .

  --- Principals
  op a : -> Name . --- Alice
  op b : -> Name . --- Bob
  op i : -> Name . --- Intruder

 --- Associativity operator
  op _;_ : Msg  Msg  -> Msg [gather (e E) frozen] .

endfm

fmod PROTOCOL-EXAMPLE-ALGEBRAIC is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .

  ----------------------------------------------------------
  --- Overwrite this module with the algebraic properties
  --- of your protocol
  ----------------------------------------------------------

  var Z : Msg .
  var Ke : Key .

  *** Encryption/Decryption Cancellation
  eq pk(Ke,sk(Ke,Z)) = Z [nonexec metadata "variant"] .
  eq sk(Ke,pk(Ke,Z)) = Z [nonexec metadata "variant"] .

endfm

fmod PROTOCOL-SPECIFICATION is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .
  protecting DEFINITION-PROTOCOL-RULES .
  protecting DEFINITION-CONSTRAINTS-INPUT .

  ----------------------------------------------------------
  --- Overwrite this module with the strands
  --- of your protocol
  ----------------------------------------------------------

  var Ke : Key .
  vars X Y Z : Msg .
  vars r r' : Fresh .
  vars A B : Name .
  vars N N1 N2 : Nonce .

  eq STRANDS-DOLEVYAO
   = :: nil :: [ nil | -(X), -(Y), +(X ; Y), nil ] &
     :: nil :: [ nil | -(X ; Y), +(X), nil ] &
     :: nil :: [ nil | -(X ; Y), +(Y), nil ] &
     :: nil :: [ nil | -(X), +(sk(i,X)), nil ] &
     :: nil :: [ nil | -(X), +(pk(Ke,X)), nil ] &
     :: nil :: [ nil | +(A), nil ]
  [nonexec] .

  eq STRANDS-PROTOCOL
   = :: r ::
     [ nil | +(pk(B,A ; n(A,r))), -(pk(A,n(A,r) ; N)), +(pk(B, N)), nil ] &
     :: r ::
     [ nil | -(pk(B,A ; N)), +(pk(A, N ; n(B,r))), -(pk(B,n(B,r))), nil ]
  [nonexec] .

  eq ATTACK-STATE(0)
   = :: r ::
     [ nil, -(pk(b,a ; N)), +(pk(a, N ; n(b,r))), -(pk(b,n(b,r))) | nil ]
     || n(b,r) inI, empty
     || nil
     || nil
     || nil
  [nonexec] .

  eq ATTACK-STATE(1)
   = :: r ::
     [ nil, -(pk(b,a ; N)), +(pk(a,  N ; n(b,r))), -(pk(b,n(b,r))) | nil ]
     ||  empty
     || nil
     || nil
     || never *** for authentication
     (:: r' ::
     [ nil, +(pk(b,a ; N)), -(pk(a,  N ; n(b,r))) | +(pk(b,n(b,r))), nil ]
     & S:StrandSet
     || K:IntruderKnowledge)
  [nonexec] .

endfm

--- THIS HAS TO BE THE LAST LOADED MODULE !!!!
select MAUDE-NPA .
```

F.2 Needham-Schroeder Lowe Protocol

The contents of the file describing this protocol are as follows:

```
fmod PROTOCOL-EXAMPLE-SYMBOLS is
  --- Importing sorts Msg, Fresh, Public, and GhostData
  protecting DEFINITION-PROTOCOL-RULES .
  ----------------------------------------------------------
  --- Overwrite this module with the syntax of your protocol
  --- Notes:
  --- * Sort Msg and Fresh are special and imported
  --- * Sorts must be subsorts of Msg
  --- * No sort can be a supersort of Msg
  ----------------------------------------------------------

  --- Sort Information
  sorts Name Nonce Key .
  subsort Name Nonce Key < Msg .
  subsort Name < Key .
  subsort Name < Public .

  --- Encoding operators for public/private encryption
  op pk : Key Msg -> Msg [frozen] .
  op sk : Key Msg -> Msg [frozen] .

  --- Nonce operator
  op n : Name Fresh -> Nonce [frozen] .

  --- Principals
  op a : -> Name . --- Alice
  op b : -> Name . --- Bob
  op i : -> Name . --- Intruder

 --- Associativity operator
  op _;_ : Msg  Msg  -> Msg [gather (e E) frozen] .

endfm

fmod PROTOCOL-EXAMPLE-ALGEBRAIC is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .

  ----------------------------------------------------------
  --- Overwrite this module with the algebraic properties
  --- of your protocol
  ----------------------------------------------------------

  var Z : Msg .
  var Ke : Key .

  *** Encryption/Decryption Cancellation
  eq pk(Ke,sk(Ke,Z)) = Z [nonexec metadata "variant"] .
  eq sk(Ke,pk(Ke,Z)) = Z [nonexec metadata "variant"] .

endfm

fmod PROTOCOL-SPECIFICATION is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .
  protecting DEFINITION-PROTOCOL-RULES .
  protecting DEFINITION-CONSTRAINTS-INPUT .

  ----------------------------------------------------------
  --- Overwrite this module with the strands
  --- of your protocol
  ----------------------------------------------------------

  var Ke : Key .
  vars X Y Z : Msg .
  vars r r' : Fresh .
  vars A B : Name .
  vars N N1 N2 : Nonce .

  eq STRANDS-DOLEVYAO
   = :: nil :: [ nil | -(X), -(Y), +(X ; Y), nil ] &
     :: nil :: [ nil | -(X ; Y), +(X), nil ] &
     :: nil :: [ nil | -(X ; Y), +(Y), nil ] &
     :: nil :: [ nil | -(X), +(sk(i,X)), nil ] &
     :: nil :: [ nil | -(X), +(pk(Ke,X)), nil ] &
     :: nil :: [ nil | +(A), nil ]
  [nonexec] .

  eq STRANDS-PROTOCOL
   = :: r ::
     [ nil | +(pk(B,A ; n(A,r))), -(pk(A,n(A,r) ; N ; B)), +(pk(B, N)), nil ] &
     :: r ::
     [ nil | -(pk(B,A ; N)), +(pk(A, N ; n(B,r) ; B)), -(pk(B,n(B,r))), nil ]
  [nonexec] .

  eq ATTACK-STATE(0)
   = :: r ::
     [ nil, -(pk(b,a ; N)), +(pk(a, N ; n(b,r) ; b)), -(pk(b,n(b,r))) | nil ]
     || n(b,r) inI, empty
     || nil
     || nil
     || nil
  [nonexec] .

endfm

--- THIS HAS TO BE THE LAST LOADED MODULE !!!!
select MAUDE-NPA .
```

F.3 Needham-Schroeder Lowe Protocol with Exclusive-or

The contents of the file describing this protocol are as follows:

```
fmod PROTOCOL-EXAMPLE-SYMBOLS is
  --- Importing sorts Msg, Fresh, Public, and GhostData
  protecting DEFINITION-PROTOCOL-RULES .

  ----------------------------------------------------------
  --- Overwrite this module with the syntax of your protocol
  --- Notes:
  --- * Sort Msg and Fresh are special and imported
  --- * Sorts must be subsorts of Msg
  --- * No sort can be a supersort of Msg
  ----------------------------------------------------------

  --- Sort Information
  sorts Name Nonce NNSet .
  subsort Name Nonce NNSet < Msg .
  subsort Name < Public .
  subsort Name Nonce < NNSet .

  --- Encoding operators for public/private encryption
  op pk : Name Msg -> Msg [frozen] .
  op sk : Name Msg -> Msg [frozen] .

  --- Concatenation operator
  op _;_ : Msg Msg -> Msg [gather (e E) frozen] .
  --- Nonce operator
  op n : Name Fresh -> Nonce [frozen] .

  --- Principals
  op a : -> Name . --- Alice
  op b : -> Name . --- Bob
  op i : -> Name . --- Intruder

 --- Exclusive or
  op _*_ : NNSet NNSet -> NNSet [assoc comm frozen] .
  op null : -> NNSet .

endfm

fmod PROTOCOL-EXAMPLE-ALGEBRAIC is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .

  ----------------------------------------------------------
  --- Overwrite this module with the algebraic properties
  --- of your protocol
  ----------------------------------------------------------

  var A : Name .
  vars X Y Z : Msg .
  vars XN YN : NNSet .

  *** Encryption/Decryption Cancellation
  eq pk(A,sk(A,Z)) = Z [metadata "variant"] .
  eq sk(A,pk(A,Z)) = Z [metadata "variant"] .

  *** Exclusive or properties
  eq XN * XN = null    [metadata "variant"] .
  eq XN * XN * YN = YN [metadata "variant"] .
  eq XN * null = XN    [metadata "variant"] .
endfm

fmod PROTOCOL-SPECIFICATION is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .
  protecting DEFINITION-PROTOCOL-RULES .
  protecting DEFINITION-CONSTRAINTS-INPUT .

  ----------------------------------------------------------
  --- Overwrite this module with the strands
  --- of your protocol
  ----------------------------------------------------------

  vars X Y Z : Msg .
  vars r r' : Fresh .
  vars A B : Name .
  vars N NA NB : Nonce .
  vars XN YN : NNSet .

  eq STRANDS-DOLEVYAO
   = :: nil :: [ nil | -(X), -(Y), +(X ; Y), nil ] &
     :: nil :: [ nil | -(X ; Y), +(X), nil ] &
     :: nil :: [ nil | -(X ; Y), +(Y), nil ] &
     :: nil :: [ nil | -(XN), -(YN), +(XN * YN), nil ] &
     :: nil :: [ nil | -(X), +(sk(i,X)), nil ] &
     :: nil :: [ nil | -(X), +(pk(A,X)), nil ] &
     :: nil :: [ nil | +(null), nil ] &
     :: r   :: [ nil | +(n(i,r)), nil ] &
     :: nil :: [ nil | +(A), nil ]
  [nonexec] .

  eq STRANDS-PROTOCOL
  = :: r ::  *** Bob ***
    [nil | +(pk(B, n(A,r) ; A)),
           -(pk(A, n(A,r) ; B * YN)),
           +(pk(B, YN)), nil]
    &
    :: r' :: *** Alice ***
    [nil | -(pk(B, XN ; A)),
           +(pk(A, XN ; B * n(B,r'))),
           -(pk(B,n(B,r'))), nil]
  [nonexec] .

  eq ATTACK-STATE(0)
   = :: r' :: *** Alice ***
     [nil, -(pk(b, XN ; a)),
           +(pk(a, XN ; b * n(b,r'))),
           -(pk(b, n(b,r'))) | nil]
     || n(b,r') inI, empty
     || nil
     || nil
     || nil
  [nonexec] .

endfm

--- THIS HAS TO BE THE LAST LOADED MODULE !!!!
select MAUDE-NPA .
```

F.4 Needham-Schroeder Lowe Protocol with Homomorphic Encryption over Concatenation

The contents of the file describing this protocol are as follows:

```
fmod PROTOCOL-EXAMPLE-SYMBOLS is
  --- Importing sorts Msg, Fresh, Public, and GhostData
  protecting DEFINITION-PROTOCOL-RULES .

  ----------------------------------------------------------
  --- Overwrite this module with the syntax of your protocol
  --- Notes:
  --- * Sort Msg and Fresh are special and imported
  --- * Sorts must be subsorts of Msg
  --- * No sort can be a supersort of Msg
  ----------------------------------------------------------

  --- Sort Information
  sorts Name Nonce Key .
  subsort Name Nonce Key < Msg .
  subsort Name < Key .
  subsort Name < Public .

  --- Encoding operators for public/private encryption
  op pk : Msg Key -> Msg [frozen] .

  --- Nonce operator
  op n : Name Fresh -> Nonce [frozen] .

  --- Principals
  op a : -> Name . --- Alice
  op b : -> Name . --- Bob
  op i : -> Name . --- Intruder

 --- Associativity operator
  op _;_ : Msg  Msg  -> Msg [gather (e E) frozen] .

endfm

fmod PROTOCOL-EXAMPLE-ALGEBRAIC is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .

  ----------------------------------------------------------
  --- Overwrite this module with the algebraic properties
  --- of your protocol
  ----------------------------------------------------------

  var X Y : Msg .
  var Z : Key .

  eq pk(X ; Y, Z) = pk(X, Z) ; pk(Y, Z) [nonexec label homomorphism metadata "builtin-unify"] .

endfm

fmod PROTOCOL-SPECIFICATION is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .
  protecting DEFINITION-PROTOCOL-RULES .
  protecting DEFINITION-CONSTRAINTS-INPUT .

  ----------------------------------------------------------
  --- Overwrite this module with the strands
  --- of your protocol
  ----------------------------------------------------------

  var Ke : Key .
  vars X Y Z : Msg .
  vars r r' : Fresh .
  vars A B : Name .
  vars N NA NB : Nonce .

  eq STRANDS-DOLEVYAO
   = :: nil :: [ nil | -(X), -(Y), +(X ; Y), nil ] &
     :: nil :: [ nil | -(X ; Y), +(X), nil ] &
     :: nil :: [ nil | -(X ; Y), +(Y), nil ] &
     :: nil :: [ nil | -(X), +(pk(X,Ke)), nil ] &
      :: nil :: [ nil | -(pk(X,i)), +(X), nil ] &
     :: nil :: [ nil | +(A), nil ]
 [nonexec] .

  eq STRANDS-PROTOCOL
   = :: r ::
     [ nil | +(pk(A ; n(A,r), B)), -(pk(n(A,r) ; NB ; B, A)), +(pk(NB, B)), nil ] &
     :: r ::
     [ nil | -(pk(A ; NA, B)), +(pk(NA ; n(B,r) ; B, A)), -(pk(n(B,r), B)), nil ]
  [nonexec] .

  eq ATTACK-STATE(0)
   = :: r ::
     [ nil, -(pk(a ; NA, b)), +(pk(NA ; n(b,r) ; b,a)), -(pk(n(b,r), b)) | nil ]
     || n(b,r) inI, empty
     || nil
     || nil
     || nil
  [nonexec] .

endfm

--- THIS HAS TO BE THE LAST LOADED MODULE !!!!
select MAUDE-NPA .
```

F.5 Diffie-Hellman protocol

The contents of the file describing this protocol are as follows:

```
fmod PROTOCOL-EXAMPLE-SYMBOLS is
  --- Importing sorts Msg, Fresh, Public
  protecting DEFINITION-PROTOCOL-RULES .

  ----------------------------------------------------------
  --- Overwrite this module with the syntax of your protocol
  --- Notes:
  --- * Sort Msg and Fresh are special and imported
  --- * Sorts must be subsorts of Msg
  --- * No sort can be a supersort of Msg
  ----------------------------------------------------------

  --- Sort Information
  sorts Name Nonce NeNonceSet Gen Exp Key GenvExp Secret .
  subsort Gen Exp < GenvExp .
  subsort Name NeNonceSet GenvExp Secret Key < Msg .
  subsort Exp < Key .
  subsort Name < Public . --- This is quite relevant and necessary
  subsort Gen < Public . --- This is quite relevant and necessary

  --- Secret
  op sec : Name Fresh -> Secret [frozen] .

  --- Nonce operator
  op n : Name Fresh -> Nonce [frozen] .

  --- Intruder
  ops a b i : -> Name .

  --- Encryption
  op e : Key Msg -> Msg [frozen] .
  op d : Key Msg -> Msg [frozen] .

  --- Exp
  op exp : GenvExp NeNonceSet -> Exp [frozen] .

  --- Gen
  op g : -> Gen .

  --- NeNonceSet
  subsort Nonce < NeNonceSet .
  op _*_ : NeNonceSet NeNonceSet -> NeNonceSet [frozen assoc comm] .

  --- Concatenation
  op _;_ : Msg Msg -> Msg [frozen gather (e E)] .

endfm

fmod PROTOCOL-EXAMPLE-ALGEBRAIC is
```

```
  protecting PROTOCOL-EXAMPLE-SYMBOLS .

  ----------------------------------------------------------
  --- Overwrite this module with the algebraic properties
  --- of your protocol
  ----------------------------------------------------------

  eq exp(exp(W:Gen,Y:NeNonceSet),Z:NeNonceSet)
   = exp(W:Gen, Y:NeNonceSet * Z:NeNonceSet) [metadata "variant"] .
  eq e(K:Key,d(K:Key,M:Msg)) = M:Msg [metadata "variant"] .
  eq d(K:Key,e(K:Key,M:Msg)) = M:Msg [metadata "variant"] .

endfm

fmod PROTOCOL-SPECIFICATION is
  protecting PROTOCOL-EXAMPLE-SYMBOLS .
  protecting DEFINITION-PROTOCOL-RULES .
  protecting DEFINITION-CONSTRAINTS-INPUT .

  ----------------------------------------------------------
  --- Overwrite this module with the strands
  --- of your protocol
  ----------------------------------------------------------

  vars NS1 NS2 NS3 NS : NeNonceSet .
  var NA NB N : Nonce .
  var GE : GenvExp .
  var G : Gen .
  vars A B : Name .
  vars r r' r1 r2 r3 : Fresh .
  var Ke : Key .
  vars XE YE : Exp .
  vars M M1 M2 : Msg .
  var Sr : Secret .

  eq STRANDS-DOLEVYAO =
     :: nil :: [ nil | -(M1 ; M2), +(M1), nil ] &
     :: nil :: [ nil | -(M1 ; M2), +(M2), nil ] &
     :: nil :: [ nil | -(M1), -(M2), +(M1 ; M2), nil ] &
     :: nil :: [ nil | -(Ke), -(M), +(e(Ke,M)), nil ] &
     :: nil :: [ nil | -(Ke), -(M), +(d(Ke,M)), nil ] &
     :: nil :: [ nil | -(NS1), -(NS2), +(NS1 * NS2), nil ] &
     :: nil :: [ nil | -(GE), -(NS), +(exp(GE,NS)), nil ] &
     :: r ::   [ nil | +(n(i,r)), nil ] &
     :: nil :: [ nil | +(g), nil ] &
     :: nil :: [ nil | +(A), nil ]
  [nonexec] .

  eq STRANDS-PROTOCOL =
     :: r,r' ::
     [nil | +(A ; B ; exp(g,n(A,r))),
            -(A ; B ; XE),
            +(e(exp(XE,n(A,r)),sec(A,r'))), nil] &
     :: r ::
     [nil | -(A ; B ; XE),
            +(A ; B ; exp(g,n(B,r))),
            -(e(exp(XE,n(B,r)),Sr)), nil]
  [nonexec] .

  eq EXTRA-GRAMMARS
   = (grl empty => (NS * n(a,r)) inL . ;
      grl empty => n(a,r) inL . ;
```

```
    grl empty => (NS * n(b,r)) inL . ;
    grl empty => n(b,r) inL .
    ! S2 )
[nonexec] .

eq ATTACK-STATE(0)
 = :: r ::
   [nil, -(a ; b ; XE),
         +(a ; b ; exp(g,n(b,r))),
         -(e(exp(XE,n(b,r)),sec(a,r'))) | nil]
   || empty
   || nil
   || nil
   || never
   *** Pattern for authentication
   (:: R:FreshSet ::
   [nil | +(a ; b ; XE),
          -(a ; b ; exp(g,n(b,r))),
          +(e(YE,sec(a,r'))), nil]
    & S:StrandSet || K:IntruderKnowledge)
[nonexec] .

eq ATTACK-STATE(1)
 = :: r ::
   [nil, -(a ; b ; XE),
         +(a ; b ; exp(g,n(b,r))),
         -(e(exp(XE,n(b,r)),sec(a,r'))) | nil]
   || sec(a,r') inI
   || nil
   || nil
   || nil
[nonexec] .

eq ATTACK-STATE(2)
 = :: r ::
   [nil, -(a ; b ; XE),
         +(a ; b ; exp(g,n(b,r))),
         -(e(exp(XE,n(b,r)),sec(a,r'))) | nil]
   || sec(a,r') inI
   || nil
   || nil
   || never(
   *** Avoid infinite useless path
    (:: nil ::
    [ nil | -(exp(GE,NS1 * NS2)), -(NS3),
        +(exp(GE,NS1 * NS2 * NS3)), nil ]
    & S:StrandSet || K:IntruderKnowledge)
   *** Pattern to avoid unreachable states
   (:: nil ::
    [nil | -(exp(#1:Exp, N1:Nonce)),
           -(sec(A:Name, #2:Fresh)),
           +(e(exp(#1:Exp, N2:Nonce), sec(A:Name, #2:Fresh))), nil]
    & S:StrandSet || K:IntruderKnowledge)
   *** Pattern to avoid unreachable states
   (:: nil ::
    [nil | -(exp(#1:Exp, N1:Nonce)),
        -(e(exp(#1:Exp, N1:Nonce), S:Secret)),
        +(S:Secret), nil]
    & S:StrandSet || K:IntruderKnowledge)
   *** Pattern to avoid unreachable states
   (S:StrandSet
    || (#4:Gen != #0:Gen), K:IntruderKnowledge)
```

```
     )
  [nonexec] .

endfm

--- THIS HAS TO BE THE LAST LOADED MODULE !!!!
select MAUDE-NPA .
```