Analysing the BKE-security protocol with µCRL

Citation for published version (APA):

Document status and date:
Published: 01/01/2004

Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:
• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher’s website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.

Download date: 02. Oct. 2020
Analyzing the BKE-security protocol with $\mu$CRL

Jan Friso Groote Sjouke Mauw Alexander Serebrenik
Laboratory of Quality of Software (LaQuSo), Division of Computer Science
Eindhoven University of Technology,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands.
E-mail: {J.F.Groote,S.Mauw,A.Serebrenik}@tue.nl

Abstract
The $\mu$CRL language and its corresponding tool set form a powerful methodology for the verification of distributed systems. We demonstrate its use by applying it to a well-known security protocol: the Bilateral Key Exchange protocol.

1 Introduction
Contemporary tools for the analysis of communicating processes are all essentially based on an explicit state space representation [7, 10, 12, 19, 23, 25]. In some cases specific data types have an explicit encoding (e.g. time in [10]), and in other cases compression techniques have been applied to the representation of states [7, 19]. The tools have matured to the level where systematically errors can be found in relatively small process descriptions. Applying the tools to larger and real-life systems is a continuous battle with the so-called state space explosion problem. The essence is that basically every communicating process that is analysed has more states than can be represented within such tools. The consequence is that behavioural analysis must be restricted to small instances under restricted communication scenario’s.

By proceeding along the current lines a steady progress can be expected. Computers become larger and faster, and better state space compression and analysis techniques will be invented. However, we are convinced that in order to make a substantial step forward, a more radical development is necessary. We believe that using the $\mu$CRL tool set [14] we made such a step.

Using techniques described in [26] it is possible to transform all $\mu$CRL processes to linear form. The tools that do this are able to perform this operation for systems consisting of hundreds of parallel processes. A linear process allows all kinds of manipulations that can easily be automated. The crucial point is that (a) human ingenuity can determine which operations must be applied and (b) computer programs are available to carry these out. A very similar situation can be found in engineering mathematics where Maple, Matlab and Mathematica have become tools to interactively manipulate large mathematical formulae. We believe it is essential that a tool set is grounded in a sound theoretical framework. For $\mu$CRL a good summary of the state of the art is given in [15].

In the current paper we will demonstrate the use of $\mu$CRL to a popular application domain, viz. the verification of security protocols. The importance of formal methods in the analysis of security protocols is evident in the fact that developing correct security protocols is notoriously difficult. Many proposed and even many implemented security protocols have been found to contain errors. The reason for this is that it is hard to predict all possible attacks that an intruder can use to break security.

The Dolev-Yao intruder model (see [9]) is the most widely accepted way of modelling an intruder. In this model the intruder has complete control over the network. He can intercept messages and construct new messages from all information that he can deduce from the messages sent by agents. The growth of the intruder knowledge, and thus the number of different messages that the intruder can construct, is the major reason for the exponential growth in the number of possible behaviours of the system.
Model checking and theorem proving are the most used formal methods for verifying security protocols. Theorem proving requires the development of a proof logic for security properties (see e.g. [6]) and in general needs user interaction. Model checking (see e.g. [20]) suffers from the state-space explosion problem, but can be done automatically. We will demonstrate the powerful state reduction techniques of the $\mu$CRL model checker by analysing the Bilateral Key Exchange (BKE, see [8]) protocol. The purpose of this protocol is to establish a fresh cryptographic key between two agents which should remain secret from a possible intruder. In order to keep our focus on the modelling of a security protocol, rather than on the modelling of security properties, we will concentrate on the secrecy requirement only.

This paper is structured as follows. In Section 2 we will explain the $\mu$CRL language and its tool set. The Bilateral Key Exchange protocol and its specification are treated in Section 3. Modelling of the he adversary is discussed in Section 4. Optimisations are the subject of Section 5. Finally, the results are evaluated in Section 6.

Acknowledgements. We thank Cas Cremers for the fruitful discussions on modelling the BKE protocol. We also thank Stefan Blom for helping us with performing the experimental evaluation.

2 A short primer in $\mu$CRL

The language $\mu$CRL (*micro Common Representation Language*) [14, 15] has been defined in 1990. At that time it had been understood that process algebras were a very suitable way to describe the behaviour of systems. Yet, process algebras did not comprise data and therefore lacked practical expressivity. With exactly this purpose in mind the languages PSF [21] and LOTOS [5] were designed. Their major goal was to make a specification language, whereas the purpose of $\mu$CRL is to constitute a practical, concise, mathematical language geared towards verification and analysis of behaviour of realistic communicating systems.

The consequence is a bare language of sufficient expressivity with a precisely defined semantics, basic axioms, proof methodology and a full range of analysis tools. In this section we shortly explain the language and the main ideas behind the verification methodologies and tools. For a much more extensive treatment, we refer to [15].

2.1 The data language

Basically, $\mu$CRL consists of a data part and a process part. The data part is built up from very simple equational abstract data types. All data sorts that are used in a specification must be declared. Sorts can be declared by

\begin{verbatim}
sort  Bool  N  List
\end{verbatim}

This declares three sorts. All sorts are non empty. The sort $\textbf{Bool}$ is special in the sense that it must have exactly two different elements denoted by $t$ and $f$. The reason for this is that terms of sort $\textbf{Bool}$ are used in conditions in process terms. Note that the difference of $t$ and $f$ can induce that other terms must be different, too. If an assumption that terms $t$ and $u$ are equal, leads to the conclusion that $f = t$, then $t$ and $u$ must be different. This technique is a form of *reductio ad absurdum* and is the only available technique in the data part of $\mu$CRL to prove that terms must be different.

Constructor functions for each sort can be declared as follows:

\begin{verbatim}
func  t, f ::= Bool
0 :→ N
succ : N → N
\end{verbatim}

We let $t$ denote true, $f$ denote false. The constructor $0$ represents zero, and $\textbf{succ}$ stands for the successor function on the natural numbers. If a sort $D$ has constructor functions with $D$ as its target sort, then all elements of that sort can be denoted using the constructor functions. Given the declaration above, $t$ and $f$ denote all booleans and each element of $\mathbb{N}$ can be written as $\textbf{succ}(\ldots(\textbf{succ}(0)\ldots))$, i.e. the application of zero or more times the application of $\textbf{succ}$ to 0.
Auxiliary functions can be defined using the keyword map. For instance the standard functions on the sort Bool can be declared as follows:

\[
\begin{align*}
\text{map} & \quad \wedge, \lor : \text{Bool} \times \text{Bool} \rightarrow \text{Bool} \\
& \quad \neg : \text{Bool} \rightarrow \text{Bool}
\end{align*}
\]

In a textual exposition we use symbols such as \(\wedge\) and \(\lor\) and use these in the normal mathematical way. The language \(\mu\text{CRL}\) which the tools can handle assume that all these functions are written in standard ASCII symbols and are all prefix. Thus a term \(t \wedge u\) is written as \`\text{and}(t, u)` to be consumable by the tool set.

Auxiliary functions do not characterise the structure of sorts. A domain \(D\) that has no constructor functions with \(D\) as target sort can in principle have any number (> 0) of elements, even uncountably many. This means that it is not possible to denote all elements of such a sort with a term.

Properties of functions can be determined by simple unconditional equations. A well-known characterisation of the functions for booleans is written as follows:

\[
\begin{align*}
\text{var} & \quad b : \text{Bool} \\
\text{rew} & \quad t \wedge b = b \\
& \quad f \wedge b = f \\
& \quad t \lor b = t \\
& \quad f \lor b = b \\
& \quad \neg t = f \\
& \quad \neg f = t
\end{align*}
\]

With the keyword var variables are declared to be used in the equations. The keyword rew comes from the verb rewrite and was chosen because rewriting technology was considered the way to prove data terms in \(\mu\text{CRL}\) equal. This term is somewhat misleading. Despite the abundant use of rewriting technology in the tools, the equations following the keyword rew must be considered as a set of plain unordered equations. Its meaning does not change if left and right hand side of an equation is exchanged or if the relative position of each equation in the rew section is altered.

This is basically all to know about the data part of \(\mu\text{CRL}\). Despite its simplicity, the language has proven itself totally apt for the specification of all conceivable data types. Its conciseness has a few advantages, namely that the data specification language can be quickly and easily understood and that building tools for it is a relatively easy affair, allowing to concentrate on making the tools very efficient.

There are also disadvantages, namely that basic data types must be defined for each specification. The extra work that it induces is not the real problem. The real problem is the lack of standardisation that it stimulates, i.e. before understanding the intricacies of a process, first the particular way the data types have been defined for this specification must be studied. This also hampers the development of meta knowledge on the data types and the use of dedicated tools.

2.2 The process language

The process language of \(\mu\text{CRL}\) is based on the language ACP, Algebra of Communicating Processes [1], which is very similar to other process specification languages, such as for instance CCS, Calculus of Communication Processes [22]. One of the most important concepts of these languages is an action. An action is an atomic event of a process that indicates a communication with the outside world or with another process. In the last case this communication takes place synchronously and is also called an interaction. Actions are typically written as \(a, b, c\) but can also have more comprehensive names such as timeout, send and receive.

Using the two main operators, namely a dot for sequential composition and a plus for alternative composition, behaviour of systems can be denoted. The process term \(a \cdot b \cdot c\) indicates the process that can consecutively perform actions \(a, b\) and \(c\). The process \(a \cdot b + c \cdot d\) indicates the process that can perform either an action \(a\) followed by an action \(b\), or an action \(c\) followed by an action \(d\). The choice between the two is made when the first action takes place. The sequential composition operator binds the strongest and is often omitted if the meaning becomes clear from the context.
Using the alternative composition operator nondeterministic processes can be described. For instance the process $a \cdot b + a \cdot c$ can initially do an $a$ action. But it is undetermined whether it would be able to do a $b$ or a $c$ action afterwards. Expressing nondeterminism is of great value. It allows to abstractly describe processes of which the actual behaviour depends on factors that cannot sufficiently, concisely or conveniently be described.

A special action, denoted by $\tau$, is called the internal action. It is an action that cannot directly be observed, for instance because it takes place inside a computer or because it represents a communication between two processes that has been shielded from observers. In order to indicate that actions are shielded the hiding operator $\tau_I$ where $I$ is a set of actions can be used. The process $\tau_{\{a,c\}}(a \cdot b \cdot c)$ equals the process $\tau \cdot b \cdot \tau$. The actions $a$ and $c$ are hidden.

There is a special process called inaction or deadlock, which is denoted as $\delta$. This is the process that cannot perform any activity. It is used for several purposes. For instance, if it is shown that a process behaves as deadlock, this is often an indication that there is something terribly wrong with the interaction between processes. In order to declare that actions cannot take place, the encapsulation operator $\partial_H$ with $H$ a set of actions is used. The process $\partial_{\{a,c\}}(a \cdot b \cdot c)$ equals $\delta \cdot b \cdot \delta$. And because $\delta$ satisfies the process equation $\delta \cdot x = \delta$, this process equals $\delta$.

The parallel operator is another feature of the language. The process $a \cdot b \parallel c \cdot d$ says that the actions $a \cdot b$ and $c \cdot d$ can be executed in any order (as long as $a$ is before $b$ and $c$ before $d$). This is called interleaving. In general, if $p$ and $q$ are processes, $p \parallel q$ denotes the process where the actions of $p$ can happen concurrent to the actions of $q$ in an interleaved fashion.

Using a communication declaration it can be indicated how actions can communicate. So, if $a$, $b$ and $c$ are actions

\[
\text{comm } a \parallel b = c
\]

indicates that the actions $a$ and $b$ in two parallel processes can happen synchronously, and the result is called $c$. So, to be explicit, the process $a \parallel b$ behaves as $a \cdot b + b \cdot a + c$. In general, synchronisation must be enforced, i.e. it is not desirable that in $a \parallel b$, the actions $a$ and $b$ can still happen in isolation. The encapsulation operator $\partial_H$ explained above can be used to block the actions $a$ and $b$. More concretely, $\partial_{\{a,b\}}(a \parallel b)$ behaves as $c$.

Although we have not yet explained the combination of processes with data, it is useful to know that actions can carry data arguments. A communication between actions can only take place if the data arguments are exactly the same. Furthermore, for multi-party communication, the communication declaration must be commutative and associative. Consult [13] for precise details.

In order to specify iterative behaviour, process equations are used. A process equation of the form

\[
X = a \cdot X
\]

indicates that a process $X$ can perform action $a$ and then behave as $X$ again. In other words, the process $X$ can perform an infinite sequence of $a$ actions. More complex equations can be written down. The process equation $Y = a \cdot Y \cdot b + c$ characterises a process that can do an arbitrary number of $a$’s, a $c$ and then as many $b$’s as it performed $a$’s. The process equation $Z = a \cdot (b \parallel Z)$ characterises a process that can continually execute $a$’s and $b$’s where the number of executed $b$’s never exceeds the number of $a$’s that took place.

2.3 Processes combined with data

The essence of $\mu$CRL is that data and processes have been combined. This boils down to four extensions of the process language.

The first extension is that actions can have data. Actions must be declared indicating which data they must have. Assuming the existence of the data sorts $\text{Bool}$ and $\mathbb{N}$ this can be done as follows:

\[
\text{act } a : \text{Bool} \times \mathbb{N} \\
a, b : \mathbb{N} \\
c
\]
Here, three actions are declared. The action \( a \) must carry either two parameters of sorts \( \text{Bool} \) and \( \mathbb{N} \), or one of sort \( \mathbb{N} \). The action \( b \) has a parameter of sort \( \mathbb{N} \) and the action \( c \) has no parameters.

The second extension is that data can be used in process equations. Formally spoken, the process variables now become higher order variables, which induces a whole world of mathematical complexity to the language. However, from a practical perspective, these equations resemble procedure declarations in standard programming language, and their use does not impose any problem.

The data is simply added to the process variable. So, a simple counter can be described as follows:

```plaintext
proc Count(n:N) = up·Count(succ(n))
```

The third extension is needed to let the data influence the flow of events. Therefore the conditional operator \( \text{then-if-else} \), denoted by \( \forall \Rightarrow \exists \) is added to the language. To show its use, we can extend the counter above to also count down. The function \( \text{pred} \) subtracts one.

```plaintext
proc Count(n:N) = up·Count(succ(n)) +
               down·Count(pred(n)) <n>0> δ
```

This process has two summands, separated by a \(+\). Both summands indicate actions that can occur independently. The \( δ \) at the else branch of the condition indicates that if \( n = 0 \) no action can be performed in the second summand.

The fourth extension is the sum operator, which in a particular case can look as follows \( \sum_{n:N} a(n) \). This indicates a choice between actions \( a(n) \) for all \( n \). This is the same as writing \( a(0) + a(succ(0)) + a(succ(succ(0))) + \cdots \). However using the binary operator \(+\) it is not possible to indicate a choice between an infinite number of options. This is exactly what the sum operator has been designed to do.

Just as an illustration, we can extend the counter above with a set action, that allows to set the counter to any arbitrary value.

```plaintext
proc Count(n:N) = up·Count(succ(n)) +
               down·Count(pred(n)) <n>0> δ +
               \( \sum_{m:N} \text{set}(m) \cdot \text{Count}(m) \)
```

Observe that the sum operator acts as binder, similarly to the \( \lambda \) in the lambda calculus, or quantifiers \( \exists, \forall \) in logic.

Except for a few rarely used constructs, we have seen all language elements of the \( \mu \text{CRL} \) language. A useful feature that has not been indicated yet, is the \text{init} keyword, using which the initial state is indicated. For the counter this could work as follows:

```plaintext
init Count(0)
```

### 2.4 Theory and tools

The \( \mu \text{CRL} \) tool set consists of a number of tools that have been used to transform and optimise the \( \mu \text{CRL} \) specification of the protocol, and to generate the state space. Names of the tools are given in italics.

The most important tool, called \text{mcrl}, checks whether a specification is a well-formed \( \mu \text{CRL} \) expression. In addition, it transforms the specification to a linear process format. In essence this format consists of a vector of data parameters, encoding the state of the process, and a set of condition-action-effect rules. These rules say under which condition on the data vector the action can be executed. The effect part of the rules indicate how the data must be updated when executing the action.

The linear process format does not contain any parallelism. Parallel operators can be translated away, without substantially blowing up the size of linear processes. The standardized linear form makes it easy to define and implement reduction and analysis tools to manipulate and understand processes.

A series of such reduction tools is applied to simplify the transformed program. One of the tools, called \text{constelm} eliminates parameters constant through any run of the process. A similar tool, \text{parelm}, removes
parameters that do not influence the behaviour of the system. For instance, in the following definition $P(x;\mathbb{N}) = a \cdot P(\text{succ}(x))$ the parameter $x$ is superfluous and can be removed. The tool \texttt{rewr} simplifies data terms in the linear process by rewriting them using the equations of the data types. The tool \texttt{structelm} replaces a term with a constructor as head symbol by a name of the constructor and its arguments. Finally, \texttt{sunelm} replaces a variable which are bound by a summation by a data term if the variable is invariantly equal to this data term. For example, $\sum_{d:B} \sum_{f:F} \text{read}(d,f) \cdot Q(d,e) \triangleleft f = e \triangleright \delta$ is transformed to $\sum_{d:B} \text{read}(d,e) \cdot Q(d,e)$. To improve the effect of the transformations some of them can be repeated. The tool \texttt{tfbupdate} replaces action labels in a linear process by others according to some translation le. In Appendix B such a le can be found, prescribing for instance that an action $c_i(t)$ for any term $t$ is replaced by an action $ctau$ without parameters. The tool \texttt{stategraph} makes a high level analysis of the dependencies between the parameters in states, and makes adaptions to reduce the state space and to make parelm and constelm more effective. These adaptions preserve the behaviour of the process in the sense of strong bisimulation.

The main purpose of the simplifications above is improving the speed of the \texttt{instantiator}, a tool generating the state space. Reducing the execution time of the instantiator is essential, since it takes lion’s share of the total execution time. In our tests the instantiator has been invoked with the following parameters: \texttt{monitor}, allowing us to keep track of the instantiator progress, and \texttt{trace NOT\_SECRET}, reporting whether the action \texttt{NOT\_SECRET} corresponding to security violation has been performed. Each test has been performed twice: with \texttt{confluent} flag and without it. This flag forces the instantiator to attempt proving that certain actions can be performed in an arbitrary order as their result does not depend on the particular execution order. In such a case, states connected by a confluent hidden action can be identified.

### 3 Bilateral Key Exchange protocol with public keys

As explained in the introduction, the goal of the Bilateral Key Exchange protocol is that two parties agree upon a freshly generated secret key. In this section we will explain this protocol in detail and discuss the \mu\text{CRL} specification of the protocol.

Figure 1 shows this protocol in a Message Sequence Chart. The two vertical axes represent the two roles of the protocol, which are the initiator role $I$ and the responder role $R$. We list the initial knowledge of each of the roles above the headers of the roles. Thus, the initiator has an asymmetric key pair $(SKi, PKi)$ and knows the public key of the responder $PKr$. Likewise, the responder has asymmetric key pair $(SKr, PKr)$ and knows the public key of some initiator $PKr$. The way in which this initial knowledge was established is not made explicit.

The initiator starts by creating a fresh nonce $ni$. This is a random, unpredictable value which is used to make the exchanged messages unique and thus helps to counter replay attacks. The first message sent by the initiator consists of the pair $ni,I$ which is encrypted with the public key of the intended responder, denoted by $\{ni,I\}_{PKr}$. Encryption is used to guarantee that only the intended recipient can unpack the message. The only messages that the responder accepts have a form $\{ni,I\}_{PKr}, i.e., they are encrypted by his public key, and they contain a nonce and the identity of the initiator. Upon receipt of the message, the responder creates his own fresh nonce $nr$ and a fresh symmetric key $kir$ that he wants to share with the initiator. The goal of the protocol is to transfer this key to the initiator in a secret way. Therefore, the responder replies with the message $\{h(ni), nr, kir\}_{PKi}$. With this message he proves that he was able to unpack the previous message (by showing that he knows nonce $ni$, witnessed by sending a hash $h(ni)$ of this nonce). Furthermore, this message contains the key $kir$ and a challenge $nr$. The complete message is encrypted with the public key of the initiator to ensure that only $I$ can unpack the message. As above, this is the only type of messages accepted by the initiator. Finally, the initiator responds to $R$’s message by sending a hash of nonce $nr$ encrypted with key $kir$. Herewith he acknowledges receipt of the previous message. At the end of the two roles we have listed the security claims as a special kind of event. Both participants claim that whenever they reach the end of their protocol the value of $kir$ cannot be known to an intruder.

A system executing this protocol consists of a number of agents, each of which may execute one or more instances of both roles (in parallel). When an agent executes a role from a protocol, we call this a run. Therefore, a system consists of a collection of runs exchanging messages to each other.
The specification of the protocol in µCRL is rather straightforward and is given in Table 1. We require data sorts Agent, natural numbers (\(\mathbb{N}\)), Nonce and Key. Agents can play different roles simultaneously. To distinguish these roles, each role gets a unique natural number \(n\). Moreover, both roles get an initial agent \(a\) with whom the role wants to establish a symmetric key. We use \(s_I\) \((s_R)\) and \(r_I\) \((r_R)\) to denote sending and receiving messages by the initiator (responder), respectively. The specification is quite straightforward and directly follows the message sequence chart.

**Table 1: Specification of the Initiator and Responder role**

\[
\begin{align*}
\text{proc } I(\text{self}:\text{Agent}, n: \mathbb{N}, a: \text{Agent}) &= \text{ } \\
& s_I(\{\text{nonce}(n), \text{addr}(\text{self})\} \text{PK}(a)) \cdot \\
& \sum_{nr: \text{Nonce}, key: \text{Key}} r_I(\{h(\text{nonce}(n)), nr, key\} \text{PK}(\text{self})) \cdot \\
& s_I(\{h(nr)\} \text{key}) \\
\text{proc } R(\text{self}:\text{Agent}, n: \mathbb{N}, a: \text{Agent}) &= \text{ } \\
& \sum_{ni: \text{Nonce}, a: \text{Agent}} r_R(\{ni, \text{addr}(a)\} \text{PK}(\text{self})) \cdot \\
& s_R(\{h(ni), \text{nonce}(n), \text{K}(n)\} \text{PK}(\text{self})) \cdot \\
& r_R(\{h(\text{nonce}(n))\} \text{K}(a))
\end{align*}
\]
4 The intruder

In order to verify correctness of the protocol we need to extend the \( \mu \text{CRL} \) specification above by adding an intruder. As explained before, we assume the so-called Dolev-Yao intruder model (see [9]), which is considered the most general model of an adversary. This model implies that the intruder has complete control over the network and that he can derive new messages from his initial knowledge and messages received from honest agents. Hereby we assume that the intruder can only decrypt messages if he is in possession of the appropriate cryptographic key. Furthermore, we assume that a number of agents may conspire with the intruder and try to mislead the honest agents as to learn their secrets. Due to the capabilities of the intruder to intercept any sent message and to insert any message which can be constructed from his knowledge, we can model the existence of conspiring agents by assuming that their secret keys are in the initial knowledge of the intruder.

Now we come back to the Bilateral Key Exchange protocol. The specification from Figure 1 is correct if for any number of agents, executing any number of runs, in the presence of a Dolev-Yao intruder, whenever an honest run enters a secrecy claim, the corresponding key \( k_{ir} \) is never exposed to the intruder.

To verify the protocol the system executes in parallel a number of runs of the initiator, a number of runs of the responder and exactly one run of the intruder. Every run is identified by an agent performing it and a number. Communication between the parties proceeds along four communication channels: from the initiator to the intruder, from the intruder to the initiator, from the responder to the intruder and from the intruder to the responder. In other words, the initiator (the responder) sends messages by performing action \( s_E(s_I) \) and reads them by performing action \( r_E(r_I) \) (cf. Table 1). Unlike them, the intruder broadcasts messages to all agents (action \( s_E \)) and reads any messages present (action \( r_E \)). Communication is possible only between \( s_E \) and \( r_I \), \( s_E \) and \( r_R \), \( s_I \) and \( r_E \), and \( s_R \) and \( r_E \). In particular, this means that the intruder gets access to all messages circulating in the network.

We also assume that the intruder can always compute the hash function \( h \) but given the value \( h(x) \) he cannot find \( x \).

In order to start the Bilateral Key Exchange protocol every participating run should know the name of the partner with whom it intends to share the secret. To implement this we require the following preparatory step to be performed: the intruder chooses the identity of the partner for each run and sends it to the corresponding agent. Agents use this information to choose public keys for encryption. It should be noted that, generally speaking, this decision could have been made by the agents themselves. However, delegating this to the intruder makes the process \( \tau \)-confluent [16] and significantly reduces a number of states. Hence, specifications presented in Table 1 are extended by a preliminary step of reading a name of the intended partner.

Finally, we review different actions that can be performed by the intruder. First of all, it listens on the incoming channels and every time a message arrives, the intruder’s knowledge is updated. At each moment of time it consists of two lists: a list of an unencrypted information obtained, and a list of pending messages waiting for decryption. Initially the first list contains addresses of all the agents, their public keys, the secret key of the intruder self and one nonce. One can show that one nonce is sufficient to simulate an intruder having infinitely many nonces. The second list is initially empty. Every time a new message is read, the intruder checks whether it has the corresponding key for decryption. If this is the case the message is decrypted, its contents is added to the list of unencrypted information and the intruder tries to use the contents to decrypt additional messages pending. If the message cannot be decrypted it is simply added to the list of pending messages. To simplify the retrieval of messages given a decryption key we organise the pending messages list as a list of \((\text{key}, \text{lom})\)-pairs, where \( \text{lom} \) is a list of messages that require \( \text{key} \) for decryption.

Next, the intruder can claim that the secrecy has been violated, if he possesses some information that has been claimed to be secret by one of the other parties. Finally, he can send a number of different messages:

1. Identity of the agent and a natural number \( p \). This message is used to establish the partner for the run identified by \( p \).
2. An unchanged message received at one of the previous steps.
3. A message imitating the first message of the initiator. It encrypts a nonce and an address.
4. A message imitating the message of the responder. It encrypts a hash of a nonce, a nonce and a symmetric key.

5. A message imitating the second message of the initiator. It contains a hash of a nonce encrypted by a symmetric key.

5 Optimisation and state space generation

Recall that in order to verify the protocol we need to generate the state space. To reduce the size of the state space a number of optimisations have been performed. The first optimisation consists of the use of types, i.e., we assume that a nonce can be always distinguished from an address, etc. Formally, we introduce four types of entities (data sorts): nonces, addresses, symmetric keys, and functional keys. The latter group includes asymmetric keys and hashes. This means that instead of two lists (unencrypted information and pending messages) at each moment of time the intruder has to remember six different lists: four corresponding to four different types of (unencrypted) entities and two lists of pending messages: those encrypted by symmetric keys and those encrypted by functional keys.

Second, scrutinising the protocol we observe that the hash function is applied exclusively to nonces, and that security claims are performed only on symmetric keys.

Third, if the responder communicates with a compromised agent, the last communication step can be omitted. Indeed, it neither changes the knowledge of the adversary, nor can it lead to an additional security claim of the responder.

Fourth, we keep track of a number of steps the intruder can perform. Each initiator or responder run can perform at most three read and send actions in the original Bilateral Key Exchange protocol and one more read action during the preliminary step. In other words, given a number of processes $n$ there is no need for the intruder to send more than $4n$ messages.

The final group of the optimisations considers the preliminary step. First of all, a number of messages during this step is limited by the number of participating processes. Hence, we add a new parameter $p$ to our implementation of the intruder. We initialise $p$ by the number of participating processes and decrement it at each iteration.

Next, recall that in order for a secrecy claim to be made the correspondent of a run should be different from the intruder. Since we are interested in finding secrecy violations, we require that the correspondent of at least one run is not the intruder. We enforce this by requiring that the last considered run ($p = 1$) communicates with a trusted party.

The last optimisation makes use of the particular form of the verification tests. Our first assumption is that there are three different agents: the one that performs the role of the intruder ($E$), the one that performs the role of the initiator ($A$) and the one that performs the role of the responder ($B$). Observe that the protocol is essentially symmetric, i.e., it is of no importance whether the initiator run performed by $A$ with the identifier 1 communicates with $B$ and the initiator run performed by $A$ with the identifier 3 communicates with $E$ or vice versa. Hence, we can order the agents ($E < A < B$) and impose the requirement that communication partners of the initiator runs of the same agent increase with respect to this ordering. The same can be said for the respondent runs of the same agent. To implement this observation we added two more parameters to our implementation of the intruder, namely $al$ and $ar$, such that the communication partner intended for an initiator (a responder) run should be greater or equal to $al$ ($ar$). In our tests, processes with odd numbers were performed by agent $A$ and played the initiator role, while processes with even numbers were performed by $B$ and played the responder role. Hence, even($p$) allows the intruder to distinguish between initiator and responder runs.

The following fragment of the intruder implementation summarises the discussion above:
6 Experimental evaluation

In this section we evaluate our approach experimentally. To do so, we have performed a series of tests. In these tests two questions have been studied. First, we were interested in the feasibility of our approach in terms of the state space size. Second, the impact of confluence on the state space size has been considered. To do so, we have performed five groups of tests: without confluence elimination on a stand-alone machine, with dynamic confluence elimination on a stand-alone machine, with static confluence elimination of a stand-alone machine, with dynamic confluence elimination on a parallel system and with static confluence elimination on a parallel system. The stand-alone machine had an Intel® Xeon CPU 2.40GHz processor with 4GB memory running Linux version 2.4.20. As a parallel system dual Athlon MP1600 nodes were used1.

Tests of the following form have been performed for a number of processes ranging from one to nine:

\[ \mu \text{CRL tools have been applied to produce the state space and to verify correctness of the protocol is represented in Table 4. The } \mu \text{CRL implementation of the BKE and the update file can be found in Appendices A and B. The following should be observed. The tool } \text{structelm} \text{ is called to expand the sort } \text{Message}. \text{ This is the sort implementing a number of different kinds of messages circulating in the network. In combination with } \text{rewr-case structelm} \text{ allows the system to distinguish between them and to generate simplified expressions for each one of the cases.} \]

It is well known [16] that confluent sets of transitions can be used to trim the state space. We aimed to understand the significance of the space reduction introduced by confluence exploration. Hence, for each run

\[ \hat{d}_{\{\tau_E, \tau_l, \tau_r, \sigma, \tau_l, \tau_r, \text{secret}, \text{secret}\_l\}} \text{ (I(A, 1) } \parallel \text{ R(B, 2) } \parallel \text{ I(A, 3) } \parallel \text{ R(B, 4) } \parallel \ldots \]  

\[ \parallel \text{ E(initialKnowledge, n, E, E) }\), \]

where \text{secret} and \text{secret\_l} are used to express the secrecy claims. Results are summarised in Table 3.

Table 2: Specification of the Intruder role (fragment)

<table>
<thead>
<tr>
<th>Machine</th>
<th>Confluence</th>
<th>Max. number of processes</th>
<th>Number of states</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand-alone</td>
<td>no</td>
<td>6</td>
<td>2094438</td>
</tr>
<tr>
<td>Stand-alone</td>
<td>dynamic</td>
<td>7</td>
<td>2223873</td>
</tr>
<tr>
<td>Stand-alone</td>
<td>static</td>
<td>8</td>
<td>14229495</td>
</tr>
<tr>
<td>Parallel</td>
<td>dynamic</td>
<td>7</td>
<td>2223873</td>
</tr>
<tr>
<td>Parallel</td>
<td>static</td>
<td>9</td>
<td>111655379</td>
</tr>
</tbody>
</table>

Table 3: Summary of results

1Tests on a parallel system have been performed by Stefan Blom at CWI.
### No confluence elimination

```
mcri -regular -nocluster -newstate security
tbfupdate -edit updatefile security | rewr | stategraph | constelm | parelm > temp0.tbf
structelm -expand Message temp0.tbf | rewr -case | sumelm |
    parelm | stategraph | constelm | parelm > temp1.tbf

time instantiator -trace NOT_SECRET -monitor temp1
```

### Static confluence elimination

```
mcri -regular -nocluster -newstate security
tbfupdate -edit updatefile security | rewr | stategraph | constelm | parelm > temp0.tbf
structelm -expand Message temp0.tbf | rewr -case | sumelm |
    parelm | stategraph | constelm | parelm > temp1.tbf

time instantiator -conluent ctau -monitor -trace NOT_SECRET temp1
```

### Dynamic confluence elimination

```
#!/bin/bash

for i in 1 2 3 4 5 6 7 8 9 10 ; do
    echo processing system$i.mcri
    m4 -DSYSTEM=System$i security24.m4 > system$i.mcri
    mcri -regular -nocluster -newstate system$i.mcri
tbfupdate -edit updatefile20 system$i.tbf | rewr | stategraph | constelm | parelm > system$i-1.tbf
    confelm system$i-1.tbf | stategraph | constelm | confelm |
```

Table 4: Tools applied
we recorded the size of the state space obtained without confluence exploration, with dynamic confluence exploration (-confluent), and static confluence elimination (confelm). As expected, the size of the state space was independent of a machine it has been generated upon. However, using a parallel system enlarged the memory size. Hence, we were able to verify the protocol for nine runs—a task for which the same algorithm on a stand-alone machine runs out of memory. Experimental results are summarised in Figure 2. Asterisks mark reference points obtained when no confluence has been explored, circles correspond to dynamic confluence elimination, and triangles to static confluence elimination. Note that a logarithmic scale is used.

![Figure 2: State spaces as function of the number of runs](image)

We observe that in all cases the state space turns out to be exponential in the number of runs. Approximation functions found by Matlab exponential fitting are $10^{1.17x-0.5647}$, $10^{0.9677x-0.6716}$, $10^{0.952x-0.5717}$ for no confluence, dynamic confluence and static confluence, respectively. These results also show that the state size reduction introduced by using confluence elimination techniques is exponential.

## 7 Conclusions

In this section we summarise the main lessons learned from our experience with implementing the BKE algorithm in µCRL and evaluating it experimentally. First of all, discovering knowledge of the experts remains a difficult task. The µCRL implementation has been modified a number of times to comply to it. Second, we have observed that general modeling tools are well-suited to verify correctness of communication protocols. Finally, our experiments suggest that eliminating confluent transactions can be essential for verification, and that static confluence elimination can outperform dynamic confluence elimination for large state spaces.

## References


A \( \mu \text{CRL-implementation of the BKE protocol} \)

% This mCRL model consists of two major parts: a data description
% and a processes description.

% First we introduce the Booleans including the basic operations.

sort Bool
func T, F: -> Bool
map
  and, or: Bool # Bool -> Bool
  not: Bool -> Bool
  eq: Bool # Bool -> Bool
  if: Bool # Bool # Bool -> Bool
  imply: Bool # Bool -> Bool

var x, y: Bool
rew
  and(T, x) = x
  or(T, x) = T
  imply(T, T) = T
  and(x, T) = x
  or(x, T) = T
  imply(T, F) = F
  and(x, F) = F
  or(x, F) = x
  imply(F, T) = T
  and(F, x) = F
  or(F, x) = x
  imply(F, F) = T
  eq(x, T) = x
  if(T, x, y) = x
  not(F) = T
  eq(T, x) = x
  if(F, x, y) = y
  not(T) = F
  eq(F, x) = not(x)
  if(x, y, y) = y
  eq(x, F) = not(x)

% Secondly, we require the natural numbers with 0 and the successor
% S as constructors. This means that each natural number can be
% written as S(S(...(0)...)).
% As a shorthand we allow to write digits 1, 2, etc. eq stands for
% equality, and sm for smaller than. P is the predecessor.

sort Nat
func 0: -> Nat
   S: Nat -> Nat
map
  eq: Nat # Nat -> Bool
  sm: Nat # Nat -> Bool
  plus: Nat # Nat -> Nat
  1, 2, 3, 4, 5, 6, 7, 8, 9: -> Nat
  P: Nat -> Nat

even: Nat → Bool

var n, m: Nat
rew eq(n, n) = T  
  sm(n, n) = F  
  eq(S(n), S(m)) = eq(n, m)  
  eq(0, S(m)) = F  
  sm(n, 0) = F  
  sm(S(n), S(m)) = sm(n, m)  
  plus(0, n) = n  
  plus(n, 0) = n  
  plus(n, S(m)) = S(plus(n, m))  

even(0) = T  
even(S(n)) = not(even(n))

P(S(n)) = n

1 = S(0)  
2 = S(1)  
3 = S(2)  
4 = S(3)  
5 = S(4)  
6 = S(5)  
7 = S(6)  
8 = S(7)  
9 = S(8)

% Agents. There are exactly three agents - A, B, E.
% We use an ordering on the agents which is defined as E < A < B.
% It is used to reduce the state space which is generated.

sort Agent
func A, B, E: Agent → Agent
map eq: Agent # Agent → Bool
  sm: Agent # Agent → Bool
  if: Bool # Agent # Agent → Agent

var a, a’: Agent
rew eq(a, a) = T  
  eq(A, B) = F  
  eq(B, A) = F  
  eq(A, E) = F  
  eq(B, E) = F  
  eq(E, A) = F  
  eq(E, B) = F  
  if(T, a, a’) = a  
  if(F, a, a’) = a’

sm(A, B) = T  
sm(A, E) = F  
sm(B, A) = F  
sm(B, E) = F  
sm(E, A) = T  
sm(E, B) = F

% There are two kinds of keys used in the protocol: symmetric and
% asymmetric ones (functional keys).
% Symmetric keys have form K(n) where n is a natural number.
% On symmetric keys we define equality eq and smaller than sm.

sort symKEY
map K: Nat → symKEY
  eq: symKEY # symKEY → Bool
  sm: symKEY # symKEY → Bool

var n, m: Nat
rew eq(K(n), K(m)) = eq(n, m)
  sm(K(n), K(m)) = sm(n, m)

% A nonce is a random, unpredictable value which is used to make the
% exchanged messages unique and thus helps to counter replay attacks.
\textbf{A \ }\mu\text{CRL-IMPLEMENTATION OF THE BKE PROTOCOL}  \hspace{1cm} 16

\begin{verbatim}
sort NONCE
map nonce:Nat\to NONCE
  eq:NONCE\#NONCE\to \text{Bool}
  sm:NONCE\#NONCE\to \text{Bool}

var n,m:Nat
rew eq(nonce(n),nonce(m)) = eq(n,m)
  sm(nonce(n),nonce(m)) = sm(n,m)

\% Address is either addr(a) for some agent a or
\% a special value badAddr, which is required to make address:funKEY\to ADDR
\% to a total function (see below). We require again the equality and
\% smaller than functions.

sort ADDR
map addr:Agent\to ADDR
  badAddr:\to ADDR
  eq:ADDR\#ADDR\to \text{Bool}
  sm:ADDR\#ADDR\to \text{Bool}

var a1,a2:Agent
rew eq(badAddr,badAddr) = F
  eq(badAddr,addr(a2)) = F
  eq(addr(a1),badAddr) = F
  eq(addr(a1),addr(a2))= eq(a1,a2)

  sm(badAddr,badAddr) = F
  sm(badAddr,addr(a2)) = T
  sm(addr(a1),addr(a2))= sm(a1,a2)
  sm(addr(a1),badAddr) = F

\% The sort funKEY contains the second kind of keys, functional keys.
\% Functional keys are public keys (PK) and secret keys (SK). Furthermore,
\% functional keys can be the result of applying a hash function (h) to
\% some nonce. For a public key k, the function decode_key returns the
\% corresponding secret key. For a given secret key, it returns the
\% corresponding public key. Otherwise decode_key returns a special value
\% NOKEY. For a public key, the function address returns the address of the
\% owner of the key. Otherwise it returns a special value badAddr.
\% The constant NOKEY is needed to make decodeKEY:funKEY\to funKEY to a
\% total function as stated above.

sort funKEY
map PK,SK:Agent\to funKEY
  h:NONCE\to funKEY
  eq:funKEY\#funKEY\to \text{Bool}
  sm:funKEY\#funKEY\to \text{Bool}
  decodeKEY:funKEY\to funKEY
  address:funKEY\to ADDR
  NOKEY :\to funKEY

var a1,a2:Agent
n1,n2: NONCE
rew eq(NOKEY,NOKEY) = T
  eq(PK(a1),NOKEY) = F
\end{verbatim}
\[
\begin{align*}
\text{eq}(\text{NOKEY}, \text{PK}(a2)) &= F & \text{eq}(\text{PK}(a1), \text{PK}(a2)) &= \text{eq}(a1, a2) \\
\text{eq}(\text{NOKEY}, \text{SK}(a2)) &= F & \text{eq}(\text{PK}(a1), \text{SK}(a2)) &= F \\
\text{eq}(\text{NOKEY}, \text{h}(n2)) &= F & \text{eq}(\text{PK}(a1), \text{h}(n2)) &= \text{F} \\
\text{eq}(\text{SK}(a1), \text{NOKEY}) &= F & \text{eq}(\text{h}(n1), \text{NOKEY}) &= F \\
\text{eq}(\text{SK}(a1), \text{PK}(a2)) &= F & \text{eq}(\text{h}(n1), \text{h}(n2)) &= \text{eq}(n1, n2) \\
\text{eq}(\text{SK}(a1), \text{SK}(a2)) &= \text{eq}(a1, a2) & \text{eq}(\text{h}(n1), \text{SK}(a1)) &= F \\
\text{sm}(\text{NOKEY}, \text{NOKEY}) &= F & \text{sm}(\text{PK}(a1), \text{NOKEY}) &= F \\
\text{sm}(\text{NOKEY}, \text{PK}(a2)) &= T & \text{sm}(\text{PK}(a1), \text{PK}(a2)) &= \text{sm}(a1, a2) \\
\text{sm}(\text{NOKEY}, \text{SK}(a2)) &= T & \text{sm}(\text{PK}(a1), \text{SK}(a2)) &= T \\
\text{sm}(\text{NOKEY}, \text{h}(n2)) &= T & \text{sm}(\text{PK}(a1), \text{h}(n2)) &= \text{T} \\
\text{sm}(\text{SK}(a1), \text{NOKEY}) &= F & \text{sm}(\text{h}(n1), \text{NOKEY}) &= F \\
\text{sm}(\text{SK}(a1), \text{PK}(a2)) &= F & \text{sm}(\text{h}(n1), \text{h}(n2)) &= \text{sm}(n1, n2) \\
\text{sm}(\text{SK}(a1), \text{SK}(a2)) &= \text{sm}(a1, a2) & \text{sm}(\text{h}(n1), \text{SK}(a1)) &= F \\
\text{sm}(\text{SK}(a1), \text{h}(n2)) &= T & \text{sm}(\text{h}(n1), \text{PK}(a1)) &= F \\
\text{decodeKEY}(\text{PK}(a1)) &= \text{SK}(a1) & \text{address}(\text{PK}(a1)) &= \text{addr}(a1) \\
\text{decodeKEY}(\text{SK}(a1)) &= \text{PK}(a1) & \text{address}(\text{h}(n1)) &= \text{badAddr} \\
\text{decodeKEY}(\text{h}(n1)) &= \text{NOKEY} & \text{address}(\text{SK}(a1)) &= \text{badAddr} \\
\text{decodeKEY}(\text{NOKEY}) &= \text{NOKEY} & \text{address}(\text{NOKEY}) &= \text{badAddr}
\end{align*}
\]

% The eavesdropper’s knowledge (see sort Knowledge below) consists of
% six different lists of information. One of them is a sorted list of
% symmetric keys obtained by the intruder, given in the sort symKEYList.
% Initially the list is empty. The function add adds a new element to
% the list, isIn is a membership test (required only for keys).
% The expression get(n,l) gets the n’th symmetric key of the symmetric
% key list l

sort symKEYList
func emptysymKEYList:->symKEYList
insymKEY:symKEY#symKEYList->symKEYList
map add:symKEY#symKEYList->symKEYList
isIn:symKEY#symKEYList->Bool
isInAUX:Bool#symKEY#symKEYList->Bool
if:Bool#symKEYList#symKEYList->symKEYList
length:symKEYList->Nat
get:Nat#symKEYList->symKEY
initialsymKEYList:->symKEYList

var k1,k2:symKEY
l1,l2:symKEYList
n:Nat
rew add(k1,emptysymKEYList)=insymKEY(k1,emptysymKEYList)
add(k1,insymKEY(k2,l1))=
\[
\begin{align*}
\text{if}(& \text{sm}(k1,k2), \text{insymKEY}(k1,\text{insymKEY}(k2,l1))
\text{if}(& \text{eq}(k1,k2), \text{insymKEY}(k2,l1),
\text{insymKEY}(k2,\text{add}(k1,l1)))
\end{align*}
\]
isIn(k1,emptysymKEYList)=F
isIn(k1,insymKEY(k2,l1))=
\begin{verbatim}
if(sm(k1,k2),F,isInAUX(eq(k1,k2),k1,l1))

isInAUX(T,k1,l1) = T
isInAUX(F,k1,l1) = isIn(k1,l1)

if(T,l1,l2)=l1
if(F,l1,l2)=l2

length(emptysymKEYList)=0
length(insymKEY(k1,l1))=S(length(l1))

g(0,insymKEY(k1,l1))=k1
g(S(n),insymKEY(k1,l1))=g(n,l1)

initialsymKEYList = emptysymKEYList

% A sorted list of nonces is also a part of the eavesdropper's knowledge.
% Initially the eavesdropper possesses one nonce. One can show that
% this is sufficient to simulate an eavesdropper with infinitely many
% nonces.

sort NONCELList
func emptyNONCELList:->NONCELList
inNONCE:NONCE#NONCELList->NONCELList
map add:NONCE#NONCELList->NONCELList
if:Bool#NONCELList#NONCELList
length:NONCELList->Nat
get:Nat#NONCELList->NONCE
initialNONCELList:->NONCELList

var k1,k2:NONCE
l1,l2:NONCELList
n:Nat

rew add(k1,emptyNONCELList)=inNONCE(k1,emptyNONCELList)
add(k1,inNONCE(k2,l1))=
  if(sm(k1,k2),inNONCE(k1,inNONCE(k2,l1)),
    if(eq(k1,k2),inNONCE(k2,l1),
      inNONCE(k2,add(k1,l1))))

if(T,l1,l2)=l1
if(F,l1,l2)=l2

length(emptyNONCELList)=0
length(inNONCE(k1,l1))=S(length(l1))

g(0,inNONCE(k1,l1))=k1
g(S(n),inNONCE(k1,l1))=g(n,l1)

initialNONCELList = add(nonce(0), emptyNONCELList)

% A sorted list of addresses is also a part of intruder's knowledge.
% All addresses are public. Hence, the initial knowledge of the
% intruder consists of the addresses of all the agents.

sort ADDRList
\end{verbatim}
A \( \mu \text{CRL}-\text{IMPLEMENTATION OF THE BKE PROTOCOL} \)

\[
\text{func emptyADDRList:}\rightarrow\text{ADDRList}
\]
\[
\text{inADDR:ADDR}\#\text{ADDRList}\rightarrow\text{ADDRList}
\]
\[
\text{map add:ADDR}\#\text{ADDRList}\rightarrow\text{ADDRList}
\]
\[
\text{if:Bool}\#\text{ADDRList}\#\text{ADDRList}\rightarrow\text{ADDRList}
\]
\[
\text{length:ADDRList}\rightarrow\text{Nat}
\]
\[
\text{get:Nat}\#\text{ADDRList}\rightarrow\text{ADDR}
\]
\[
\text{initialADDRList:}\rightarrow\text{ADDRList}
\]

\[
\text{var k1,k2:ADDR}
\]
\[
\text{n:Nat}
\]
\[
\text{rew add(k1,emptyADDRList)=inADDR(k1,emptyADDRList)}
\]
\[
\text{add(k1,inADDR(k2,l1))=}
\]
\[
\text{if(sm(k1,k2),inADDR(k1,inADDR(k2,l1))},
\]
\[
\text{if(eq(k1,k2),inADDR(k2,l1)},
\]
\[
\text{inADDR(k2,add(k1,l1))})
\]
\[
\text{if(T},l1,l2)=l1
\]
\[
\text{if(F},l1,l2)=l2
\]
\[
\text{length(emptyADDRList)=0}
\]
\[
\text{length(inADDR(k1,l1))=S(length(l1))}
\]
\[
\text{get(0},inADDR(k1,l1))=k1
\]
\[
\text{get(S(n)},inADDR(k1,l1))=get(n,l1)
\]
\[
\text{initialADDRList= add(addr(A), add(addr(B),}
\]
\[
\text{add(addr(E)},emptyADDRList))}
\]

\[
\%\text{The intruder also keeps a sorted list of functional keys.}
\%
\]
\[
\%\text{Initially all public keys are known to the intruder. And}
\%
\]
\[
\%\text{naturally the eavesdropper initially knows its own}
\%
\]
\[
\%\text{secret key.}
\%
\]
\[
\text{sort funKEYList}
\]
\[
\text{func emptyfunKEYList:}\rightarrow\text{funKEYList}
\]
\[
\text{infunKEY:funKEY}\#\text{funKEYList}\rightarrow\text{funKEYList}
\]
\[
\text{map add:funKEY}\#\text{funKEYList}\rightarrow\text{funKEYList}
\]
\[
\text{isIn:funKEY}\#\text{funKEYList}\rightarrow\text{Bool}
\]
\[
\text{isInAUX:Bool}\#\text{funKEY}\#\text{funKEYList}\rightarrow\text{Bool}
\]
\[
\text{if:Bool}\#\text{funKEYList}\#\text{funKEYList}\rightarrow\text{funKEYList}
\]
\[
\text{length:funKEYList}\rightarrow\text{Nat}
\]
\[
\text{get:Nat}\#\text{funKEYList}\rightarrow\text{funKEY}
\]
\[
\text{initialfunKEYList:}\rightarrow\text{funKEYList}
\]

\[
\text{var k1,k2:funKEY}
\]
\[
\text{n:Nat}
\]
\[
\text{rew add(k1,emptyfunKEYList)=infunKEY(k1,emptyfunKEYList)}
\]
\[
\text{add(k1,infunKEY(k2,l1))=}
\]
\[
\text{if(sm(k1,k2),infunKEY(k1,infunKEY(k2,l1))},
\]
\[
\text{if(eq(k1,k2),infunKEY(k2,l1)},
\]
\[
\text{infunKEY(k2,add(k1,l1))})
\]
\[
\text{isIn(k1,emptyfunKEYList)=F}
\]
isIn(k1,infunKEY(k2,l1))=
   if(sm(k1,k2),F,isInAUX(eq(k1,k2),k1,l1))

isInAUX(T,k1,l1) = T
isInAUX(F,k1,l1) = isIn(k1,l1)

if(T,l1,l2)=l1
if(F,l1,l2)=l2

length(emptyfunKEYList)=0
length(infunKEY(k1,l1))=S(length(l1))

get(0,infunKEY(k1,l1))=k1
get(S(n),infunKEY(k1,l1))=get(n,l1)

initialfunKEYList = add(PK(A), add(PK(B),
   add(PK(E), add(SK(E), emptyfunKEYList))))

% The sort Message contains all the messages that are exchanged
% in the BKE protocol. There three kinds of messages:
% two sent by the initiator and one sent by the responder.
% The second message sent by an initiator consists of a functional
% key encrypted by a symmetric key. The first message sent by an
% initiator contains a nonce and an address encrypted by a
% functional key. The message sent by the receiver contains a
% functional key, a nonce, a symmetric key and it is encrypted by
% a functional key. The functions get... are projections to extract
% information from the messages.
% The functions encryptedN (N=1,2,3) indicate whether a message
% has a particular form. The function encrypted1 is true if its
% first argument has the form of the second I-message and the key
% used during the encryption is its second argument.
% The function encrypted2 is true if its first argument has the form
% of the first I-message and the key used during the encryption
% is its second argument. The function encrypted3 is true if its
% first argument has the form of the R-message and the key used
% during the encryption is its second argument. Two messages are equal,
% expressed using the function eq iff they are of the same kind
% and all components are equal.
% The function sm defines an ordering on messages. This ordering is
% defined as follows:
% for any fk1,sk2,n1,a2,fk3,fk1',n2,sk3 and fk4
%    encrypt(fk1,sk2) < encrypt(n1,a2,fk3) < encrypt(fk1',n2,sk3,fk4).
% Messages of the same kind are compared lexicographically.

sort Message
func encrypt:funKEY#symKEY->Message
   encrypt:NONCE#ADDR#funKEY->Message
   encrypt:funKEY#NONCE#symKEY#funKEY->Message
map eq:Message#Message->Bool
get1N:Message->NONCE
get1f:Message->funKEY
get2N:Message->NONCE
get2A:Message->ADDR
\[\text{get3s: Message} \rightarrow \text{symKEY}\]
\[\text{sm: Message} \rightarrow \text{Bool}\]
\[\text{encrypted1: Message} \rightarrow \text{symKEY} \rightarrow \text{Bool}\]
\[\text{encrypted2: Message} \rightarrow \text{funKEY} \rightarrow \text{Bool}\]
\[\text{encrypted3: Message} \rightarrow \text{funKEY} \rightarrow \text{Bool}\]

\[\text{var} \quad f_{k1}, f_{k1}', f_{k3}, f_{k3}', f_{k4}, f_{k4}', f_{k5} : \text{funKEY}\]
\[\quad s_{k2}, s_{k2}', s_{k3}, s_{k3}', s_{k4}, s_{k5} : \text{symKEY}\]
\[\quad n_1, n_1', n_2, n_2' : \text{NONCE}\]
\[\quad a_2, a_2' : \text{ADDR}\]

\[\text{rew} \]
\[\text{eq(encrypt}(f_{k1}, s_{k2}), \text{encrypt}(n_1', a_2', f_{k3}'))= F\]
\[\text{eq(encrypt}(f_{k1}, s_{k2}), \text{encrypt}(f_{k1}', n_2', s_{k3}', f_{k4}'))= F\]
\[\text{eq(encrypt}(n_1, a_2, f_{k3}), \text{encrypt}(f_{k1}', s_{k2}'))= F\]
\[\text{eq(encrypt}(f_{k1}, s_{k2}), \text{encrypt}(f_{k1}', s_{k2}'))= F\]
\[\text{eq(encrypt}(n_1, a_2, f_{k3}), \text{encrypt}(n_1', a_2', f_{k3}'))= F\]
\[\text{eq(encrypt}(f_{k1}, s_{k2}), \text{encrypt}(f_{k1}', s_{k2}'))= F\]

\[\text{get1f(encrypt}(f_{k1}, s_{k2}))= f_{k1}\]
\[\text{get1f(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}))= f_{k1}\]
\[\text{get1N(encrypt}(n_1, a_2, f_{k3}))= n_1\]
\[\text{get2A(encrypt}(n_1, a_2, f_{k3}))= a_2\]
\[\text{get2N(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}))= n_2\]
\[\text{get3s(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}))= s_{k3}\]

\[\text{sm(encrypt}(f_{k1}, s_{k2}), \text{encrypt}(f_{k1}', s_{k2}'))=\]
\[\quad \text{or(} \text{sm}(f_{k1}, f_{k1}'),\]
\[\quad \quad \land(\text{eq}(f_{k1}, f_{k1}'), \text{sm}(s_{k2}, s_{k2}')))\]
\[\text{sm(encrypt}(f_{k1}, s_{k2}), \text{encrypt}(n_1', a_2', f_{k3}'))= T\]
\[\text{sm(encrypt}(f_{k1}, s_{k2}), \text{encrypt}(f_{k1}', n_2', s_{k3}', f_{k4}'))= T\]
\[\text{sm(encrypt}(n_1, a_2, f_{k3}), \text{encrypt}(f_{k1}', s_{k2}'))= F\]
\[\text{sm(encrypt}(n_1, a_2, f_{k3}), \text{encrypt}(n_1', a_2', f_{k3}'))= F\]
\[\text{sm(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}), \text{encrypt}(f_{k1}', s_{k2}'))= F\]
\[\text{sm(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}), \text{encrypt}(n_1', a_2', f_{k3}'))= F\]
\[\text{sm(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}), \text{encrypt}(f_{k1}', n_2', s_{k3}', f_{k4}'))=\]
\[\quad \text{or(} \text{sm}(f_{k1}, f_{k1}'),\]
\[\quad \quad \land(\text{eq}(f_{k1}, f_{k1}'), \text{sm}(f_{k3}, f_{k3}')))\]
\[\text{sm(encrypt}(n_1, a_2, f_{k3}), \text{encrypt}(f_{k1}', n_2', s_{k3}', f_{k4}'))= T\]
\[\text{sm(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}), \text{encrypt}(f_{k1}', s_{k2}'))= F\]
\[\text{sm(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}), \text{encrypt}(n_1', a_2', f_{k3}'))= F\]
\[\text{sm(encrypt}(f_{k1}, n_2, s_{k3}, f_{k4}), \text{encrypt}(f_{k1}', n_2', s_{k3}', f_{k4}'))=\]
\[\quad \text{or(} \text{sm}(f_{k1}, f_{k1}'),\]
\[\quad \quad \land(\text{eq}(f_{k1}, f_{k1}'), \text{sm}(s_{k3}, s_{k3}')))\]
\[\text{sm(encrypt}(n_1, a_2, f_{k3}), \text{encrypt}(f_{k1}', n_2', s_{k3}', f_{k4}'))= T\]
\[
\mu \text{CRL-IMPLEMENTATION OF THE BKE PROTOCOL}
\]

\[
\text{encrypted1}(\text{encrypt}(f_k1, s_k2), s_k3) = \text{eq}(s_k2, s_k3)
\]

\[
\text{encrypted1}(\text{encrypt}(n_1, a_2, f_k3), s_k4) = \text{F}
\]

\[
\text{encrypted1}(\text{encrypt}(f_k1, n_2, s_k3, f_k4), s_k5) = \text{F}
\]

\[
\text{encrypted2}(\text{encrypt}(f_k1, s_k2), f_k3) = \text{F}
\]

\[
\text{encrypted2}(\text{encrypt}(n_1, a_2, f_k3), f_k4) = \text{eq}(f_k3, f_k4)
\]

\[
\text{encrypted2}(\text{encrypt}(f_k1, n_2, s_k3, f_k4), f_k5) = \text{F}
\]

\[
\text{encrypted3}(\text{encrypt}(f_k1, s_k2), f_k3) = \text{F}
\]

\[
\text{encrypted3}(\text{encrypt}(n_1, a_2, f_k3), f_k4) = \text{F}
\]

\[
\text{encrypted3}(\text{encrypt}(f_k1, n_2, s_k3, f_k4), f_k5) = \text{eq}(f_k4, f_k5)
\]

% The sort MessageList contains sorted list of messages obtained by
% the intruder. It has the same operations as the lists of nonces
% and addresses. We do not store the messages directly in the intruder’s
% knowledge but distinguish between those encoded by symmetric keys and
% and those encoded by the functional keys (see ConditionalfunKEYList and
% ConditionalsymKEYList below).

sort MessageList

func emptyMessageList:->MessageList
inMessage:Message#MessageList->MessageList
map add:Message#MessageList->MessageList
if:Bool#MessageList#MessageList->MessageList
length:MessageList->Nat
get:Nat#MessageList->Message

var m1,m2:Message
l1,l2:MessageList
n:Nat
rew add(m1,emptyMessageList)=inMessage(m1,emptyMessageList)
add(m1,inMessage(m2,l1))=
if(sm(m1,m2),inMessage(m1,inMessage(m2,l1)),
  if(eq(m1,m2),inMessage(m2,l1),
    inMessage(m2,add(m1,l1))))
if(T,l1,l2)=l1
if(F,l1,l2)=l2

length(emptyMessageList)=0
length(inMessage(m1,l1))=S(length(l1))

get(0,inMessage(m1,l1))=m1
get(S(n),inMessage(m1,l1))=get(n,l1)

% The sort funEncaps is an auxiliary sort, needed in ConditionalfunKEYList.
% It represents a pair of (ConditionalfunKEYList,MessageList).

sort funEncaps

func encaps:ConditionalfunKEYList#MessageList->funEncaps
map pr1: funEncaps->ConditionalfunKEYList
pr2: funEncaps->MessageList
if:Bool#funEncaps#funEncaps->funEncaps
\[ \text{var } fcl:\text{ConditionalfunKEYList} \\
\quad \text{ml:MessageList} \\
\quad \text{fe1,fe2:funEncaps} \\
\text{rew } \text{pr1}(\text{encaps}(fcl,ml)) = fcl \\
\text{pr2}(\text{encaps}(fcl,ml)) = ml \\
\quad \text{if}(\text{T},\text{fe1},\text{fe2})=\text{fe1} \\
\quad \text{if}(\text{F},\text{fe1},\text{fe2})=\text{fe2} \]

\% The list of the messages received by the intruder that are indexed by 
\% functional keys is given in the sort \text{ConditionalFunKEYList}. The list has 
\% the form \(<fak1,l1,fk2,l2,\ldots>\) where each \(l_i\) is a list of messages 
\% received so far that are encrypted by the preceding 
\% functional key \(f^k_i\). The function \text{addCond} adds a pair \((\text{funKEY},\text{Message})\) 
\% to an existing list \text{ConditionalfunKEYList} and returns an updated list. 
\% The function \text{removeCond} removes messages encoded by \text{funKEY} from the 
\% list \text{ConditionalfunKEYList}. It returns a pair encoded by the sort 
\% \text{funEncaps}: an updated list \text{ConditionalfunKEYList} and a list of messages 
\% corresponding to \text{funKEY} in the original list. If no messages encoded 
\% by \text{funKEY} are present, it returns an unchanged list \text{ConditionalfunKEYList} 
\% and an empty list of messages. The second equation for the function 
\% \text{addCond} is quite complex. It makes a distinction between the values of 
\% \(k_1\) and \(k_2\). If \(k_1<k_2\) then \((k_1,m)\) should be added at the front of the 
\% list of messages. If \(k_1 = k_2\) then the intruder has already some 
\% messages encrypted by \(k_1\). Therefore, \(m\) has to be added to the 
\% corresponding list of messages. If \(k_1>k_2\) then, since the list is 
\% ordered, we proceed with adding \((k,m)\) to its tail. A similar distinction 
\% is made for \text{removeCond}. 

\text{sort\text{ConditionalfunKEYList}} \\
\text{func emptyCfunKEYList:->ConditionalfunKEYList} \\
\quad \text{inCfunKEY:funKEY#MessageList#ConditionalfunKEYList->} \\
\quad \quad \text{ConditionalfunKEYList} \\
\text{map addCond:funKEY#Message#ConditionalfunKEYList->} \\
\quad \quad \text{ConditionalfunKEYList} \\
\text{removeCond:funKEY#ConditionalfunKEYList->funEncaps} \\
\text{if:Bool#ConditionalfunKEYList#ConditionalfunKEYList->} \\
\quad \quad \text{ConditionalfunKEYList} \\
\text{getMessageList:Nat#ConditionalfunKEYList->MessageList} \\
\text{length:ConditionalfunKEYList->Nat} \\

\text{var } k1,k2:funKEY \\
\quad m:Message \\
\quad L:MessageList \\
\quad CL,CL1:ConditionalfunKEYList \\
\quad n:Nat \\
\text{rew addCond}(k1,m,\text{emptyCfunKEYList})= \\
\quad \text{inCfunKEY}(k1,\text{inMessage}(m,\text{emptyMessageList}), \\
\quad \quad \text{emptyCfunKEYList}) \\
\text{addCond}(k1,m,\text{inCfunKEY}(k2,L,CL))= \\
\quad \text{if}(\text{sm}(k1,k2), \\
\quad \quad \text{inCfunKEY}(k1,\text{inMessage}(m,\text{emptyMessageList}),\text{inCfunKEY}(k2,L,CL)), \\
\quad \quad \text{if}(\text{eq}(k1,k2), \\
\quad \quad \text{inCfunKEY}(k2,\text{add}(m,L),CL), \\
\quad \quad \text{inCfunKEY}(k2,L,\text{addCond}(k1,m,CL))))


\[\text{removeCond}(k_1, \text{emptyCfunKEYList}) = \text{encaps}(\text{emptyCfunKEYList}, \text{emptyMessageList})\]

\[\text{removeCond}(k_1, \text{inCfunKEY}(k_2, L, CL)) = \begin{cases} 
\text{if}(\text{sm}(k_1, k_2), \\
\text{encaps}(CL, \text{emptyMessageList}), \\
\text{if}(\text{eq}(k_1, k_2), \\
\text{encaps}(CL, L), \\
\text{encaps}(\text{inCfunKEY}(k_2, L, \text{pr1(removeCond}(k_1, CL))), \text{pr2(removeCond}(k_1, CL)))))
\end{cases}\]

\[\text{if}(T, CL, CL_1) = CL\]
\[\text{if}(F, CL, CL_1) = CL_1\]

\[\text{length}(\text{emptyCfunKEYList}) = 0\]
\[\text{length}(\text{inCfunKEY}(k_1, L, CL)) = S(\text{length}(CL))\]

\[\text{getMessageList}(n, \text{emptyCfunKEYList}) = \text{emptyMessageList}\]
\[\text{getMessageList}(0, \text{inCfunKEY}(k_1, L, CL)) = L\]
\[\text{getMessageList}(S(n), \text{inCfunKEY}(k_1, L, CL)) = \text{getMessageList}(n, CL)\]

% The sort symEncaps is also auxiliary, similar to funEncaps.

\text{sort} symEncaps

\text{func} \text{encaps}: \text{ConditionalsymKEYList}\#\text{MessageList} -> \text{symEncaps}

\text{map} \text{pr1}: \text{symEncaps} -> \text{ConditionalsymKEYList}
\text{pr2}: \text{symEncaps} -> \text{MessageList}

\text{if}: \text{Bool}\#\text{symEncaps}\#\text{symEncaps} -> \text{symEncaps}

\text{var} fcl: \text{ConditionalsymKEYList}
ml: \text{MessageList}
se1, se2: \text{symEncaps}

\text{rew} \text{pr1(encaps}(fcl, ml)) = fcl
\text{pr2(encaps}(fcl, ml)) = ml
\text{if}(T, se1, se2) = se1
\text{if}(F, se1, se2) = se2

% The sort ConditionalsymKEYList contains a list of messages received
% en that have been encoded by symmetric keys. For
% explanations see ConditionalfunKEYList above, which has exactly
% the same structure.

\text{sort} ConditionalsymKEYList

\text{func} \text{emptyCsymKEYList}: -> \text{ConditionalsymKEYList}
\text{inCsymKEY}: \text{symKEY}\#\text{MessageList}\#\text{ConditionalsymKEYList} -> 
\text{ConditionalsymKEYList}

\text{map} \text{addCond}: \text{symKEY}\#\text{Message}\#\text{ConditionalsymKEYList} -> 
\text{ConditionalsymKEYList}
\text{removeCond}: \text{symKEY}\#\text{ConditionalsymKEYList} -> \text{symEncaps}
\text{if}: \text{Bool}\#\text{ConditionalsymKEYList}\#\text{ConditionalsymKEYList} -> 
\text{ConditionalsymKEYList}
\text{getMessageList}: \text{Nat}\#\text{ConditionalsymKEYList} -> \text{MessageList}
\text{length}: \text{ConditionalsymKEYList} -> \text{Nat}

\text{var} k_1, k_2: \text{symKEY}
\[ \text{addCond}(k_1, m, \text{emptyCsymKEYList}) = \]
\[ = \text{inCsymKEY}(k_1, \text{inMessage}(m, \text{emptyMessageList}), \]
\[ \text{emptyCsymKEYList}) \]
\[ \text{addCond}(k_1, m, \text{inCsymKEY}(k_2, L, CL)) = \]
\[ = \begin{cases} \text{inCsymKEY}(k_1, \text{inMessage}(m, \text{emptyMessageList}), \text{inCsymKEY}(k_2, L, CL)), & \text{if } \text{sm}(k_1, k_2) \text{,} \\ \text{if } \text{eq}(k_1, k_2), \text{inCsymKEY}(k_2, \text{add}(m, L), CL), \text{inCsymKEY}(k_2, L, \text{addCond}(k_1, m, CL))) & \end{cases} \]
\[ \text{removeCond}(k_1, \text{emptyCsymKEYList}) = \]
\[ = \text{encaps}(\text{emptyCsymKEYList}, \text{emptyMessageList}) \]
\[ \text{removeCond}(k_1, \text{inCsymKEY}(k_2, L, CL)) = \]
\[ = \begin{cases} \text{encaps}(CL, \text{emptyMessageList}), & \text{if } \text{sm}(k_1, k_2), \\ \text{if } \text{eq}(k_1, k_2), \text{encaps}(CL, L), \text{encaps}(\text{inCsymKEY}(k_2, L, pr1(\text{removeCond}(k_1, CL))), pr2(\text{removeCond}(k_1, CL)))) & \end{cases} \]
\[ \text{if}(T, CL, CL1) = CL \]
\[ \text{if}(F, CL, CL1) = CL1 \]
\[ \text{length} (\text{emptyCsymKEYList}) = 0 \]
\[ \text{length} (\text{inCsymKEY}(k_1, L, CL)) = S(\text{length}(CL)) \]
\[ \text{getMessageList}(n, \text{emptyCsymKEYList}) = \text{emptyMessageList} \]
\[ \text{getMessageList}(0, \text{inCsymKEY}(k_1, L, CL)) = L \]
\[ \text{getMessageList}(S(n), \text{inCsymKEY}(k_1, L, CL)) = \text{getMessageList}(n, CL) \]

% The sort Knowledge of the intruder. This sort implements the entire
% knowledge of the intruder, consisting of six different lists: two
% lists of messages (encoded by symmetric and functional keys), and
% lists of symmetric keys, functional keys, nonces and addresses. The
% most important function of this sort is updateKnowledge that given
% a (list of) message(s) and the current state of intruder’s knowledge
% updates it and returns the updated state of knowledge. Updating knowledge
% is a recursive process since decrypting a message can result in obtaining
% new symmetric or functional keys that in their turn can be used to
% decrypt further messages. This propagation step is modeled by two
% auxiliary functions propagates and propagatelf.

sort Knowledge
func wrap:ConditionalsymKEYList#ConditionalfunKEYList#
symKEYList#funKEYList#NONCEList#ADDRList->Knowledge
map fEncMessages: Knowledge->ConditionalfunKEYList
sEncMessages: Knowledge->ConditionalsymKEYList
fKEYs: Knowledge->funKEYList
sKEYs: Knowledge->symKEYList
addresses: Knowledge->ADDRList
nonces: Knowledge->NONCEList
if:Bool#Knowledge#Knowledge->Knowledge
updateKnowledge:Message#Knowledge->Knowledge
updateKnowledge:MessageList#Knowledge->Knowledge
propagates:symKEY#Knowledge->Knowledge
propagatesf:funKEY#Knowledge->Knowledge
initialKnowledge:->Knowledge

var scl: ConditionalsymKEYList
fcl: ConditionalfunKEYList
s1: symKEYList
f1: funKEYList
nl: NONCEList
al: ADDRList
K1,K2:Knowledge
f,f1:funKEY
s:symKEY
n:NONCE
a:ADDR
ml:MessageList
m: Message

rew sEncMessages(wrap(scl,fcl,s1,f1,nl,al)) = scl
fEncMessages(wrap(scl,fcl,s1,f1,nl,al)) = fcl
sKEYs(wrap(scl,fcl,s1,f1,nl,al)) = s1
fKEYs(wrap(scl,fcl,s1,f1,nl,al)) = f1
addresses(wrap(scl,fcl,s1,f1,nl,al)) = al
nonces(wrap(scl,fcl,s1,f1,nl,al)) = nl
if(T,K1,K2) = K1
if(F,K1,K2) = K2

updateKnowledge(encrypt(f,s),wrap(scl,fcl,s1,f1,nl,al)) =
  if(isIn(s,sl),
    propagatef(f,wrap(scl,fcl,s1,add(f,f1),nl,al)),
    wrap(addCond(s,encrypt(f,s),scl),fcl,s1,f1,nl,al))
updateKnowledge(encrypt(n,a,f),wrap(scl,fcl,s1,f1,nl,al)) =
  if(isIn(decodeKEY(f),fl),
    wrap(scl,fcl,s1,f1,add(n,nl),add(a,al)),
    wrap(scl,addCond(f,encrypt(n,a,f),fcl),s1,f1,nl,al))
updateKnowledge(encrypt(f1,n,s,f),wrap(scl,fcl,s1,f1,nl,al)) =
  if(isIn(decodeKEY(f),fl),
    propagates(s,
      propagatef(f1,
        wrap(scl,fcl,add(s,s1),add(f1,f1),add(n,nl),al))),
      wrap(scl,addCond(f,encrypt(f1,n,s,f),fcl),s1,f1,nl,al))
updateKnowledge(emptyMessageList,K1) = K1
updateKnowledge(inMessage(m,ml),K1) =
  updateKnowledge(ml,updateKnowledge(m,K1))
propagates(s,wrap(scl,fcl,s1,f1,nl,al)) =
  updateKnowledge(pr2(removeCond(s,scl)),
    wrap(pr1(removeCond(s,scl)),fcl,s1,f1,nl,al))
propagatesf(f,wrap(scl,fcl,s1,f1,nl,al)) =
\begin{verbatim}
updateKnowledge(pr2(removeCond(f,fcl)),
    wrap(scl,pr1(removeCond(f,fcl)),s1,f1,n1,al))

initialKnowledge =
    wrap(emptyCsymKEYList,emptyCfunKEYList,
        initialsymKEYList, initialFunKEYList,
        initialNONCEList, initialADDRList)

% Here we are finished with the required datatypes. Below we
% define the processes. We start out with declaring the actions
% that the processes use to communicate. Using the comm declaration
% section, it is defined how these action communicate. Then we
% model three processes, the initiator, the responder and the
% eavesdropper (Iproc, Rproc and Eproc). Then we define different
% constellations of initiators, responder and eavesdroppers that
% we have analysed. The concrete selection is made using the
% keyword init at the end.

act sE :Message % send of the eavesdropper.
    sE :Agent#Nat % send of the eavesdropper
        % (the preliminary step).
    rE :Message % receive of the eavesdropper.
    sI :Message % send of the initiator.
    rI :Message % receive of the initiator.
    rI :Agent#Nat % receive of the initiator
        % (the preliminary step).
    sR :Message % send of the responder.
    rR :Message % receive of the responder.
    rR :Agent#Nat % receive of the responder
        % (the preliminary step).
    c1,c2,c3,c4:Message % communication between sends
        % and receives. See "comm" below.
    c2,c4 :Agent#Nat % communication between sends and
        % receives. See "comm" below
        % (the preliminary step).
    secret :symKEY % secrecy claims of the initiator
        % and the responder.
    secret_ :symKEY % the receipt of a claim by the
        % eavesdropper to check whether
        % it knows the secret.
    secret__ :symKEY % communication of secrecy claims.
    NOT_SECRET % secrecy violation indicator.

% Below it is defined on which channels the different
% processes synchronize to exchange information.

comm sI|rE = c1 % from the initiator to the intruder
    sE|rI = c2 % from the intruder to the initiator
    sR|rE = c3 % from the responder to the intruder
    sE|rR = c4 % from the intruder to the responder
    secret|secret_ = secret__

% Below we model the initiator. The initiator starts by creating a
% fresh nonce. The first message sent by the initiator consists of
\end{verbatim}
% the nonce and his address encrypted with the public key of the
% intended responder. Then, the initiator reads a message, verifies %
% that it has the expected form (a functional key and a hash of a
% nonce encrypted by the initiator’s public key), and acknowledges
% receipt of the message by sending hash of the shared nonce
% encrypted by the shared symmetric key. Finally, the initiator
% claims security of the shared symmetric key. For further details
% see the main text.

proc Iproc(self:Agent,n:Nat)=
  sum(a:Agent,rI(a,n).
    sI(encrypt(nonce(n),addr(self),PK(a))).
  sum(m:Message,rI(m).
    (aI(encrypt(h(get2N(m)),get3s(m))).
      (secret(get3s(m))<| not(eq(a,E))|> delta).delta)
    <| and(encrypted3(m,PK{self}),eq(get1f(m),h(nonce(n))))|> delta

% The responder is similarly to the initiator. The responder starts
% by receiving a message, verifies that it is in the expected form
% (contains the address of the presumed counterpart encrypted by the
% responder’s public key), generates a new nonce and sends a message
% consisting of the hashed nonce of the counterpart, the newly
% created nonce and the symmetric key to be shared, encrypted by the
% public key of the counterpart. Next, the responder reads a new
% message, verifies that it has been encrypted by the shared symmetric
% key and contains the hash function of his nonce, and claims secrecy
% of the shared key. Additional information can be found in the main text.

proc Rproc(self:Agent,n:Nat)=
  sum(a:Agent,rR(a,n).
    sum(m1:Message,rR(m1).
      sR(encrypt(h(get1N(m1)),nonce(n),K(n),PK(a))).
    sum(m2:Message,rR(m2).
      secret(K(n)).delta
      <| and(not(eq(a,E)),and(encrypted1(m2,K(n)),
        eq(get1f(m2),h(nonce(n))))) |> delta
    )<| and(eq(get2A(m1),addr(a)),
      encrypted2(m1,PK{self})) |> delta
  )

% The process Eproc models the eavesdropper. The first summand (action rE)
% describes the receipt of a message. This message is immediately added to
% the knowledge that the eavesdropper already has. The next summands, except
% the last, describe the sending of an arbitrary message that can be
% constructed with the knowledge of the eavesdropper. In this way all
% possible attacks on the protocol are modelled. The last summand consists
% of receiving a supposed to be secret. If the eavesdropper knows it,
% it signals a NOT_SECRET action. Please refer to Section 4 of
% the main text for further details.

proc Eproc(K:Knowledge,p:Nat,aI:Agent,aR:Agent)=
  sum(m:Message,rE(m).Eproc(updateKnowledge(m,K),p,aI,aR)
\[
\begin{align*}
\text{sum}(a: \text{Agent},) \\
& (sE(a,p).\text{Eproc}(K,p,aI,aR)) \\
& \text{if}(\text{eq}(p,2),aI,aR) \\
& \text{and}(\text{sm}(0,p),\text{not}(\text{sm}(a,aR))) \\
& \text{delta}) + \\
\text{sum}(a: \text{Agent},) \\
& (sE(a,p).\text{Eproc}(K,p,aI,aR)) \\
& \text{if}(\text{eq}(p,1),aI,aR) \\
& \text{and}(\text{sm}(0,p),\text{not}(\text{sm}(a,aI))) \\
& \text{imp}(\text{and}(\text{eq}(p,1),\text{eq}(aI,aR))) \\
& \text{not}(\text{eq}(a,E))) \\
& \text{delta}) + \\
\text{sum}(n1: \text{Nat}) \\
& \text{sum}(n2: \text{Nat},) \\
& (sE(\text{encrypt}(h(\text{get}(n1,\text{nonces}(K))), \\
& \text{get}(n2,\text{sKEYs}(K))).\text{Eproc}(K,p,aI,aR)) \\
& \text{if}(\text{eq}(0,p),) \\
& \text{and}(\text{eq}(0,p),) \\
& \text{and}(\text{sm}(n1,\text{length}(\text{nonces}(K))),) \\
& \text{sm}(n2,\text{length}(\text{sKEYs}(K)))) \\
& \text{delta}) + \\
\text{sum}(n1: \text{Nat}) \\
& \text{sum}(n2: \text{Nat},) \\
& (sE(\text{encrypt}(\text{get}(n1,\text{fKEYs}(K)), \\
& \text{get}(n2,\text{sKEYs}(K))).\text{Eproc}(K,p,aI,aR)) \\
& \text{if}(\text{eq}(0,p),) \\
& \text{and}(\text{eq}(0,p),) \\
& \text{and}(\text{sm}(n1,\text{length}(\text{fKEYs}(K))),) \\
& \text{sm}(n2,\text{length}(\text{sKEYs}(K)))) \\
& \text{delta}) + \\
\text{sum}(n1: \text{Nat}) \\
& \text{sum}(n2: \text{Nat},) \\
& \text{sum}(n3: \text{Nat},) \\
& (sE(\text{encrypt}(h(\text{get}(n1,\text{nonces}(K))), \text{get}(n2,\text{addresses}(K)), \\
& \text{get}(n3,\text{sKEYs}(K))).\text{Eproc}(K,p,aI,aR)) \\
& \text{if}(\text{eq}(0,p),) \\
& \text{and}(\text{eq}(0,p),) \\
& \text{and}(\text{sm}(n1,\text{length}(\text{nonces}(K))),) \\
& \text{and}(\text{sm}(n2,\text{length}(\text{addresses}(K))),) \\
& \text{sm}(n3,\text{length}(\text{sKEYs}(K)))) \\
& \text{delta}) + \\
\text{sum}(n1: \text{Nat}) \\
& \text{sum}(n2: \text{Nat},) \\
& \text{sum}(n3: \text{Nat},) \\
& \text{sum}(n4: \text{Nat},) \\
& (sE(\text{encrypt}(h(\text{get}(n1,\text{nonces}(K))), \text{get}(n2,\text{nonces}(K)), \\
& \text{get}(n3,\text{sKEYs}(K)), \text{get}(n4,\text{fKEYs}(K))).\text{Eproc}(K,p,aI,aR)) \\
& \text{if}(\text{eq}(0,p),) \\
& \text{and}(\text{eq}(0,p),) \\
& \text{and}(\text{sm}(n1,\text{length}(\text{nonces}(K))),) \\
& \text{and}(\text{sm}(n2,\text{length}(\text{nonces}(K))),) \\
& \text{and}(\text{sm}(n3,\text{length}(\text{sKEYs}(K))),) \\
& \text{sm}(n4,\text{length}(\text{fKEYs}(K)))) \\
& \text{delta}) + \\
\text{sum}(n1: \text{Nat}) \\
& \text{sum}(n2: \text{Nat},) \\
& \text{sum}(n3: \text{Nat},) \\
& \text{sum}(n4: \text{Nat},) \\
& (sE(\text{encrypt}(\text{get}(n1,\text{fKEYs}(K)), \text{get}(n2,\text{nonces}(K)), \\
& \text{get}(n3,\text{sKEYs}(K)), \text{get}(n4,\text{fKEYs}(K))).\text{Eproc}(K,p,aI,aR)) \\
& \text{if}(\text{eq}(0,p),) \\
& \text{and}(\text{eq}(0,p),) \\
& \text{and}(\text{sm}(n1,\text{length}(\text{fKEYs}(K))),) \\
& \text{and}(\text{sm}(n2,\text{length}(\text{nonces}(K))),) \\
& \text{and}(\text{sm}(n3,\text{length}(\text{sKEYs}(K))),)
\end{align*}
\]
\[
\sum(n_1: \text{Nat}, \sum(n_2: \text{Nat},
\text{Eproc}(K, p, a_I, a_R)
\begin{cases}
\text{and(eq(0, p),}
\text{and(sm(n_1, length(sEncMessages(K))),}
\text{sm(n_2, length(getMessageList(n_1, sEncMessages(K)))))}
\end{cases}
\[\delta])
+ \\
\sum(n_1: \text{Nat}, \sum(n_2: \text{Nat},
\text{Eproc}(K, p, a_I, a_R)
\begin{cases}
\text{and(eq(0, p),}
\text{and(sm(n_1, length(fEncMessages(K))),}
\text{sm(n_2, length(getMessageList(n_1, fEncMessages(K)))))}
\end{cases}
\[\delta])
+ \\
\sum(k: \text{symKEY}, \text{secret}_k).
(NOT_SECRET.Eproc(K, p, a_I, a_R)
\begin{cases}
\text{isIn(k, sKEYs(K)})
\end{cases}
\[\text{Eproc(K, p, a_I, a_R)}
\])
\]
\]

% System1..System9 are used to test the protocol for 1..9 processes.
% To generate the state space: replace ‘init System5’ below by ‘init SystemN’, where N is the desired number of processes.

proc System1=
\text{encap}((rE, sI, rI, sE, rR, secret, secret_),
\text{Iproc(A, 1) ||}
\text{Eproc(initialKnowledge, 1, E, E))}

proc System2=
\text{encap}((rE, sI, rI, sE, sR, rR, secret, secret_),
\text{Iproc(A, 1) || Rproc(B, 2) ||}
\text{Eproc(initialKnowledge, 2, E, E))}

proc System3=
\text{encap}((rE, sI, rI, sE, sR, rR, secret, secret_),
\text{Iproc(A, 1) || Rproc(B, 2) ||}
\text{Iproc(A, 3) ||}
\text{Eproc(initialKnowledge, 3, E, E))}

proc System4=
\text{encap}((rE, sI, rI, sE, sR, rR, secret, secret_),
\text{Iproc(A, 1) || Rproc(B, 2) ||}
\text{Iproc(A, 3) || Rproc(B, 4) ||}
\text{Eproc(initialKnowledge, 4, E, E))}

proc System5=
\text{encap}((rE, sI, rI, sE, sR, rR, secret, secret_),
\text{Iproc(A, 1) || Rproc(B, 2) ||}
The file updatefile contains renamings of actions. E.g. in the description below the action c1(X) is renamed to ctau where X is any parameter. It is possible to formulate conditions on these parameters to perform conditional renaming. This is not used below. The tool tbfupdate is needed to carry out the actual renaming on a linear process.

- c1(X) -> ctau
- c2(X) -> tau
- c3(X) -> ctau
- c4(X) -> tau
- c2(X,Y) -> tau
- c4(X,Y) -> tau
- secret__(X) -> tau