RAPPORT TECHNIQUE EVA

Symbolic verification of cryptographic protocols with time stamps

Date	:	December 13, 2003
Authors	:	L. Bozga, C. Ene, Y. Lakhnech
Title	:	Symbolic verification of cryptographic protocols with time stamps
Report number / Version	:	12/ 1

TRUSTED LOGIC S.A.
5 rue du Bailliage
78000 Versailles, France
www.trusted-logic.fr

Laboratoire Spécification Vérification
CNRS UMR 8643, ENS Cachan
61, avenue du président-Wilson
94235 Cachan Cedex, France
www.lsv.ens-cachan.fr

Laboratoire Verimag
CNRS UMR 5104,
Univ. Joseph Fourier, INPG
2 av. de Vignate,
38610 Gières, France
www-verimag.imag.fr

Symbolic verification of cryptographic protocols with time stamps

L. Bozga, C. Ene, Y. Lakhnech

December 13, 2003

1 Introduction

Some cryptographic protocols rely upon timestamps that recipients use to verify timeliness of the message and recognize and reject replays of messages communicated in the past. Timestamps are also used in conjunction with short term keys. The presence of timestamps makes the specification and verification of cryptographic protocols a challenging problem. Indeed, most of the existing verification methods and decidability results for cryptographic protocols consider time-independent protocols [THG98, RT01, AL00, Bor01, MS01, FA01, CS02, CLC03]. Because of the subtleties and complexity of the verification of time-dependent protocols, theorem provers have been used to verify such protocols.

In this paper, we present a model for time-dependent cryptographic protocols and a corresponding decidability result. Although, the model we present only deals with bounded protocols, that is, when a fixed number of sessions are considered, our model clearly identifies the main ingredients to be included in a general model. Besides general models for distributed systems that can be used to model security protocols such as Timed CSP and MSR (multiset rewriting over first-order atomic formulae), we do not know about a model for timed cryptographic protocols.

To model timed cryptographic protocols, we include in our model clocks, time variables and timestamps. Clocks are variables that range over the time domain and advance with the same rate as time. Each agent has its own set clocks that he can reset. That is clocks can be used to measure the time that elapses between two events, for instance, sending a message and receiving the corresponding response. Also, we allow a global clock that is never reset and that can be read and tested by all participants. Time variables correspond to timestamps in received messages. Such values can be stored and used together with clocks to put conditions on the acceptance of a message.

A second contribution of this paper is a complete and sound symbolic verification algorithm for timed cryptographic protocols. We consider a rich class of reachability properties that allow to specify confidentiality and authentication. In fact, we introduce a logic that allows to describe secrecy, equalities between terms and control points. Then, given a bounded protocol Π and two formulae in this logic Φ and Ψ, the reachability problem we consider is whether there is a run of Π that starts in a configuration that satisfies Φ and reaches a configuration that satisfies Ψ.

We device a symbolic algorithm that given a property described by a formula Ψ in this logic and given a bounded protocol computes the set of configurations that reaches Ψ. This algorithm uses symbolic constraints (logic formulae) to describe sets of configurations. The logic we introduce combines constraints on the knowledge of the intruder with time constraints on clock values and time variables. To show effectiveness of our verification method we show:

1. that for each action of our model we can express the predecessor configurations of a set of configurations as a formula. We consider input, output and time actions.

2. Then, we show decidability of the satisfiability problem for our logic.

Related work Our model is clearly inspired by timed automata and our verification method influenced by the work on symbolic verification of timed automata and temporal logics for real-time systems (e.g.[AD94, HNSY92, AFH91, BL95]).

The results of this paper provide an algorithm for checking security properties (confidentiality and authentication) of timed cryptographic protocols. It has several interesting aspects:

1. it covers other properties than confidentiality (secrecy); indeed while other methods rely on an ad hoc reduction of authentication properties to secrecy, our method is directly applicable.

2. as initial configuration are described by formulae of the introduced logic, it can deal with infinite non-regular sets of messages initially known by the intruder.

3. we believe that our method is more easily amenable to extended intruder models.

Handling time constraints, unbounded message size symbolically and automatically is the distinguishing feature of our verification method. Most of the work on timed cryptographic protocols uses theorem-provers or finite-state model-checking [BP98, Coh00, ES00, Low97]. While the first needs human help, the second relies on typing assumptions and assumption on the time window to bound the search space.

2 Preliminaries

Let X be a countable set of variables and let F^i be a countable set of function symbols of arity i, for every $i \in \mathbb{N}$. Let $F = \bigcup_{i\in\mathbb{N}} F^i$. The set of *terms over X and F*, denoted by $\mathcal{T}(X, F)$. We denote by $\leq$ the *subterm* relation $\leq$ on $\mathcal{T}(X, F)$. As usual, function symbols of arity 0 are called constant symbols. *Ground terms* are terms with no variables. We denote by $\mathcal{T}(F)$ the set of ground terms over F. For any $t_1, t_2 \in \mathcal{T}(X, F)$, we denote with $\mu(t_1, t_2)$ the most general unifier (shortly mgu) of t_1 and t_2, if it exists. More precisely, by $\mu(t_1, t_2)$ we denote the representation of the mgu of t_1 and t_2 as a conjunction of equalities of the form $x = t$, if it exists. If it does not exist then $\mu(t_1, t_2)$ should be the constant $false$ (falsum). We write $t_1 \sim t_2$, if t_1, t_2 can be unified. Also, for any substitution $\sigma : X \to \mathcal{T}(X, F)$ and term $t \in \mathcal{T}(X, F)$, we denote by $dom(\sigma)$ the domain of σ and by $t\sigma$ the application to t of the homomorphic extension of σ to terms. Given a set $\tilde{x}$ of variables, we denote by $\Gamma(\tilde{x})$ the set consisting of ground substitutions with domain $\tilde{x}$. We also write $\Gamma(x)$ instead of $\Gamma(\{x\})$. Given two substitutions σ and ρ with disjoint domains, $\sigma \oplus \rho$ is the substitution equal to σ on $dom(\sigma)$, equal to ρ on $dom(\rho)$, and undefined elsewhere.

A tree tr is a function from a finite subset of ω^* to $X \cup F$ such that $tr(u) \in F^n$ iff $u \cdot j \in dom(tr)$, for every $j \in \{0, \cdots, n-1\}$. Henceforth, we tacitly identify the term t with $Tr(t)$. The elements of $dom(t)$ are called *positions* in t. We use $\prec$ to denote the prefix relation on ω^*. We write $t(p)$ to denote the symbol at position p in t and $t_{|p}$ to denote the subterm of t at position p, which corresponds to the tree $t_{|p}(x) = t(p \cdot x)$ with $x \in dom(t_{|p})$ iff $p \cdot x \in dom(t)$. Given a term t and positions p and q, we say that $t_{|p}$ dominates $t_{|q}$ if $p \prec q$.

If $w_1, w_2 \in \Sigma^*$ are words over an alphabet Σ, then we denote by $w_2^{-1}w_1$ the word obtained from w_1 after removing the prefix w_2.

3 The Protocol and Intruder Model

We describe in this section the model of cryptographic protocols adopted in this paper. We assume Dolev-Yao's intruder model except that, since we are dealing with timed protocols, we add a rule that allows the derivation of any time-stamp.

Thus, in addition to the usual terms considered in Dolev-Yao model, we add:

1. Clocks, i.e. variables that range over the underlying time model. We denote the set of clocks by $\mathcal{C}$.

2. Timestamps, that is values in the time domain.

3. Time variables, that is variables that range over the time domain. We denote by $\mathcal{Y}$ the set time variables.

It is important to understand the difference between these three disjoint sets of variables: a time stamp is just a constant; clocks and time variables are variables. The difference is that the value of a clock advances with rate one with time while the value of a time variable does not. A time variable is simply a variable that ranges over the time domain.

We fix the time domain to be the set of non-negative real numbers. Our results, however, hold also when we consider the natural numbers instead.

Let $\mathcal{X}$ denote the set of variables that range over terms. Let $\mathcal{A} = \mathcal{P} \cup \mathcal{N} \cup \mathcal{K} \cup \mathbb{R}_{\geq 0}$ and $\mathcal{F} = \mathcal{A} \cup \{\mathbf{encr}, \mathbf{pair}\}$. We consider terms build from constant symbols in $\mathcal{A}$, clocks in $\mathcal{C}$ and time variables in $\mathcal{Y}$ using the function symbols in $\mathcal{F}$. As usual, we write (m_1, m_2) for $\mathbf{pair}(m_1, m_2)$ and $\{m\}_k$ instead of $\mathbf{encr}(m, k)$. A *Clock-free term* is a term in which no clock appears; time variables and time stamps may appear in a clock-free term. We denote the set of clock-free terms by $\mathcal{T}(\mathcal{X} \cup \mathcal{Y}, \mathcal{F})$. *Messages* are ground terms in $\mathcal{T}(\mathcal{X} \cup \mathcal{Y}, \mathcal{F})$, we denote by $\mathcal{M} = \mathcal{T}(\mathcal{F})$ the set of messages. For conciseness, we write $\mathcal{T}$ instead of $\mathcal{T}(\mathcal{X} \cup \mathcal{Y}, \mathcal{F})$ and $\mathcal{T}_c$ instead of $\mathcal{T}(\mathcal{X} \cup \mathcal{Y} \cup \mathcal{C}, \mathcal{F})$.

We use the usual model of Dolev and Yao [DY83] augmented with the axiom

$$\text{If } r \in \mathbb{R}_{\geq 0} \text{ then } E \vdash r.$$

The axiom represents the fact that the intruder can guess every possible time-stamp, i.e. time value. As usual, we write $E \vdash m$, when m is derivable from E using the augmented Dolev-Yao model. A derivation of a message that does not use decomposition rules is denoted by $E \vdash_c m$. For a term t, we use the notation $E \nvdash t$ to denote that no instance of t is derivable from E, that is, for no substitution $\sigma : \mathcal{X} \to \mathcal{M}$, we have $E \vdash t\sigma$.

Given a term t, a position p in t is called *non-critical*, if there is a position q such that $p = q \cdot 2$ and $t(q) = \mathbf{encr}$; otherwise it is called *critical*. That is, encryption key positions are non-critical. We will also use the notation $s \in_c m$ to denote that s appears in m at a critical position, i.e., there exists $p \in dom(m)$ such that p is critical and $m_{|p} = s$.

3.1 Process model

Timed cryptographic protocols are build from timed actions. Here, we consider two types of actions: message input and message output. A time constraint is associated to an action and describes when the action is possible.

Definition 3.1 (time constraints) *Time constraints are defined by:*

$$g ::= \top \mid \sum_{i=1}^{n} a_i c_i + \sum_{j=1}^{m} b_j T_j \bowtie d \mid g_1 \wedge g_2 \mid g_1 \vee g_2$$

where $m, n \in \mathbb{N}$, $c_i \in \mathcal{C}$ are clocks, $T_j \in \mathcal{Y}$ are time variables , $a_i, b_j \in \mathbb{Z}$, $d \in \mathbb{Z}$, and $\bowtie \in \{<, \leq\}$. The set of time constraints is denoted by $\mathcal{TC}$.

A time constraints is interpreted with respect to a valuation ν defined over a finite set of clocks $\{c_1, \ldots, c_n\}$ that associates values in the time domain to clocks, and a substitution σ that assigns ground clock-free terms to variables. The interpretation of a time constraint is given by:

- $[\![\top]\!]_{\nu,\sigma} = 1$, for any ν and σ.
- $[\![\sum_{i=1}^{n} a_i c_i + \sum_{j=1}^{m} b_j T_j \bowtie d]\!]_{\nu,\sigma} = 1$ iff $\sum_{i=1}^{n} a_i \nu(c_i) + \sum_{j=1}^{m} b_j \sigma(T_j) \bowtie d$;
- $[\![g_1 \wedge g_2]\!]_{\nu,\sigma} = 1$ iff $[\![g_1]\!]_{\nu,\sigma} = [\![g_2]\!]_{\nu,\sigma} = 1$;
- $[\![g_1 \vee g_2]\!]_{\nu,\sigma} = 1$ iff $[\![g_1]\!]_{\nu,\sigma} = 1$ or $[\![g_2]\!]_{\nu,\sigma} = 1$

Then (ν, σ) is said to be a *model* for a time constraint g, if $[\![g]\!]_{\nu,\sigma} = 1$.

Given a time constraint g and a set $\mathcal{R}$ of clocks,we denote by $g[\mathcal{R}]$ the time constraint obtained by substituting 0 for all clocks in $\mathcal{R}$. We also use the notation $g + d$ to denote the time constraint obtained from g by substituting each clock c in g by $c + d$.

Definition 3.2 (actions and protocols) We consider input and output actions:

- **An input** action is of the form $l \xrightarrow{g,\mathcal{R},?t(\tilde{x})} l'$, where
  - $g \in \mathcal{TC}$ is a time constraint called the guard,
  - $t(\tilde{x}) \in \mathcal{T}$ is a term and $\tilde{x} \subseteq \mathcal{X} \cup \mathcal{Y}$ is the set of variables instantiated by the input action.
  - $\mathcal{R} \subseteq \mathcal{C}$ is a subset of clocks
  - l, l' are labels
- **An output** action is of the form $l \xrightarrow{g,\mathcal{R},!t_c} l'$ where g, l, l' and $\mathcal{R}$ are as above and $t_c \in \mathcal{T}_c$ is a clock dependent term.

The set of actions is denoted by $\mathcal{A}ct$.

A protocol is represented by a set of sequences of actions. More precisely, a protocol Π is given by:

$$\Pi = \sum_{i=1}^{n} \alpha_1^i \cdots \alpha_{n_i}^i.$$

where $\alpha_j^i = \ell_j^i \xrightarrow{g,\mathcal{R},\beta_j^i} \ell_{j+1}^i$ for some β_j^i with $j \in \{1, \ldots, n_i\}$. Here, the labels ℓ represent control points and $\sum$ is the usual non-deterministic choice. This corresponds to the interleavings of a fixed set of sessions put in parallel.

$$\Pi = \sum_{i=1}^{n} \ell_0^i \beta_0^i \cdots \ell_{n_i}^i \beta_{n_i}^i \ell_{n_i+1}^i.$$

Let $\mathcal{R} \subseteq \mathcal{C}$ be a subset of clocks, $\delta \in \mathbb{R}_{\geq 0}$ a constant, $\nu : \mathcal{C} \longrightarrow \mathbb{R}_{\geq 0}$ a valuation for clocks, and let $t_c \in \mathcal{T}_c$ be a clock dependent term. We denote by $\nu[\mathcal{R}]$ the valuation obtained from ν by resetting all clocks in $\mathcal{R}$, i.e. $\nu[\mathcal{R}](c) = 0$ for any $c \in \mathcal{R}$ and $\nu[\mathcal{R}](c) = \nu(c)$ for any $c \notin \mathcal{R}$; $\nu + \delta$ denotes the valuation which advances all clocks by the same delay δ, i.e. $(\nu + \delta)(c) = \nu(c) + \delta$; and $t_c[\nu]$ is the term obtained from t_c by replacing all occurrences of c by the value of $\nu(c)$.

Definition 3.3 (operational semantics) *A configuration of a protocol run is given by a tuple (σ, E, ν, ℓ) consisting of a substitution σ, a set of messages E, a valuation of clocks ν and a control point ℓ. The operational semantics is defined as a labelled transitional system over the set of configurations $\mathcal{C}onf$. The transition relation*

$$(\sigma, E, \nu, \ell) \xrightarrow{\alpha} (\sigma', E', \nu', \ell')$$

is defined as follows:

- **output:** $\alpha = \ell_j^i \xrightarrow{g,\mathcal{R},!t} \ell_{j+1}^i$. *Then, we have*

  $$(\sigma, E, \nu, \ell_j^i) \xrightarrow{\alpha} (\sigma, E', \nu', \ell_{j+1}^i)$$

  if $j \leq n_i$, $[\![g]\!]_{\nu,\sigma} = 1$, $\sigma' = \sigma$, $E' = E \cup \{t\sigma \oplus \nu[\mathcal{R}]\}$ and $\nu' = \nu[\mathcal{R}]$.

  That is, sending the message t (provided that guard g is satisfied by the actual configuration) amounts to reset clocks in $\mathcal{R}$ and adding t evaluated with respect to the substitution σ and the valuation of clocks $\nu[\mathcal{R}]$, to the knowledge of the intruder

- **input:** $\alpha = \ell_j^i \xrightarrow{g,\mathcal{R},?t(\tilde{x})} \ell_{j+1}^i$.

  Then, we have

  $$(\sigma, E, \nu, \ell_j^i) \xrightarrow{\alpha} (\sigma', E, \nu', \ell_{j+1}^i)$$

  if $j \leq n_i$ and there is $\rho \in \Gamma(\tilde{x})$ with $E\sigma \vdash t(\sigma \oplus \rho)$, $[\![g]\!]_{\nu,\sigma\oplus\rho} = 1$, $\sigma' = \sigma \oplus \rho$, and $\nu' = \nu[\mathcal{R}]$.

  That is, $?t$ corresponds to receiving any message, known to the intruder, that matches with $?t\sigma$ by a substitution ρ, such that g is satisfied by the pair ν, $\sigma \oplus \rho$; in addition, this action resets clocks in $\mathcal{R}$.

- **time passing:** $(\sigma, E, \nu, \ell^i_j) \xrightarrow{\delta} (\sigma, E, \nu + \delta, \ell^i_j)$, *for any* $\delta \in \mathbb{R}_{\geq 0}$. *This action represents the passage of* δ *time units; passage of an arbitrary time is denoted by* $\xrightarrow{\tau} = \bigcup_{\delta \in \mathbb{R}_{\geq 0}} \xrightarrow{\delta}$.

The initial configuration is given by a substitution σ_0*, a set of terms* E_0 *such that the variables in* E_0 *do not appear in the protocol description, a valuation* ν_0 *and a control point* $\ell_0 \in \{\ell^1_0, \cdots, \ell^n_{n_i}\}$.

Example 3.1 *The Denning-Sacco shared key protocol [CJ97], a protocol for distribution of a shared symmetric key by a trusted server and mutual authentication. Here, the timestamps are used to ensure the freshness of the shared key. Using the usual notation for cryptographic protocols, the protocol is described as follows:*

$$\begin{array}{ll} A \to S: & A, B \\ S \to A: & \{B, Kab, T, \{Kab, A, T\}_{Kbs}\}_{Kas} \\ A \to B: & \{Kab, A, T\}_{Kbs} \end{array}$$

The keys Kas *and* Kbs *are shared keys between the participant* A *respectively* B *and the server* S*. The goal of the Denning-Sacco shared key protocol is to allow two principals* A *and* B *to obtain a secret symmetric key from a trusted server* S*.*

The next table shows how we describe the protocol. The constant parameters δ_1*,* δ_2 *represent network delays for* A *respectively* B*. We use a special clock now which is a global clock that is never reset and has an arbitrary initial value. For convenience of notation, we write* $\ell\ \alpha\ \ell'$ *instead of* $\ell \xrightarrow{\alpha} \ell'$ *and we omit the guard when it is the constant* $\top$ *and the set of clocks to be reset when it is empty.*

A:

$0\ !(A, B)\ 1$

$1\ now - T_1 < \delta_1,\ ?\{B, x, T_1, y\}_{smk(A,S)}\ 2$

$2\ !y\ 3$

S:

$0\ ?(z, v)\ 1$

$1\ !\{v, K, now, \{K, z, now\}_{smk(v,S)}\}_{smk(z,S)}\ 2$

B:

$0\ now - T_2 < \delta_2,\ ?\{u, p, T_2\}_{smk(B,S)},\ 1$

Each participant of the protocol may be seen as a sequential process. First, the participant A *sends his identity* A *and the identity of* B *to the server. Then,* A *receives back the message* $\{B, x, T_1, y\}_{smk(A,S)}$*. If* T_1*, is a valid timestamp, that means the difference between the current time and the value of* T_1 *is less than the constant parameter* δ_1 *then* A *accepts* x *as session key and forwards the message* y *to* B*. On the other side,* B*, when receives the message* $\{u, p, T_2\}_{smk(B,S)}$*, it checks if* T_2 *is a valid timestamp with respect to the current time and, if it is, it accepts* p *as session key. The server* S*, every time when it receives a pair of two participants* (z, v) *it generates a new session key* K *and sends it together with its current time now in a message of the form* $\{v, K, now, \{K, z, now\}_{smk(v,S)}\}_{smk(z,S)}$ *to the first participant of the pair* z*.*

4 The TSPL logic

In this section, we introduce the constraints/formulae we use to describe security properties. The logic we introduce allows to describe secrecy, authentication and any safety property.

Henceforth, let $K \subseteq \mathcal{K}$ be a fixed but arbitrary set of keys, such that $\emptyset \neq K \neq \mathcal{K}$.

4.1 Term transducers and the main modality of the logic

A pair $(\{t\}_k, r)$, where t is a term, $k \in K$ and r a critical position in $\{t\}_k$ is called a *term transducer (TT for short)*. Intuitively, the pair $(\{t\}_k, r)$ can be seen as function that takes as argument a term that matches with $\{t\}_k$ and returns as result the term $\{t\}_{k_{|r}}$. Notice that the decomposition rules in the intruder model can be considered as a set of term transducers the intruder can apply to get new terms. As it will become clear later, a run of a CP provides the intruder with new term transducer she (he) can apply to learn new terms.

The main modality of the logic we use can be defined as follows:

Definition 4.1 Let m and s be two messages and let $w \in (\mathcal{M} \times \mathcal{P}os)^*$ be a sequence of term transducers. We define the predicate $m\langle w \rangle s$, which we read "s is w-protected in m", recursively on the structure of m and length of w:

- m is atomic and $m \neq s$, or
- $m = \mathbf{pair}(m_1, m_2)$, $m \neq s$ and both $m_1\langle w\rangle s$ and $m_2\langle w\rangle s$ are true, or
- $m = \mathbf{encr}(m_1, k)$, $m \neq s$, $k \notin K$ and $m_1\langle w\rangle s$ is true, or
- $m = \mathbf{encr}(m_1, k)$, $m \neq s$, $k \in K$ and $w = \epsilon$, or
- $m = \mathbf{encr}(m_1, k)$, $w = (b, r).w_1$, $m \neq s$, $k \in K$, and $m \neq b$ or $m|_r\langle w_1\rangle s$ is true.

This definition is easily generalized to sets of messages: Let M and S be sets of messages, w a sequence of term transducers and K a set of keys. We say that the secrets S are w - protected in M denoted by $M\langle w\rangle S$, if it holds $\bigwedge_{m\in M, s\in S} m\langle w\rangle s$.

Example 4.1 *Let $m = (\{A, \{N\}_{k_1}\}_{k_2}, A)$ and $K = \{k_1, k_2\}$. Then, $m\langle\epsilon\rangle N$ is true since $\{A, \{N\}_{k_1}\}_{k_2}\langle\epsilon\rangle N$ and $A\langle\epsilon\rangle N$ are true.*

Let now $w = (\{A, \{N\}_{k_1}\}_{k_2}, 12).(\{N\}_{k_1}, 1)$. Then, $m\langle w\rangle N$ is false since applying the term transducer $(\{A, \{N\}_{k_1}\}_{k_2}, 12)$ yields $\{N\}_{k_1}$ on which an application of $(\{N\}_{k_1}, 1)$ yields N.

4.1.1 Closure of sets of secrets

In this section, we define when a set of messages is closed. Closed sets of secrets enjoy the property that they are not derivable by composition. Intuitively, a set of messages is closed if it contains all messages along every path of the tree representing a message in the set. The same idea is used in e.g. [Pau97, THG98, CMR01].

Let M be a set of sets of messages and let m be a message. We use the notation: $m \odot M = \{M_i \cup \{m\} | M_i \in M\}$.

We define when a set of messages is closed. The closure of a set S ensures that the intruder cannot derive a message in S by composition rules.

Definition 4.2 (closure)

$$wc(m) = m \odot \begin{cases} wc(m1) \cup wc(m2) & \text{if } m = (m1, m2) \\ wc(m') \cup wc(k) & \text{if } m = \{m'\}_k \\ \{K^{-1}\} & \text{if } m \text{ is atomic} \end{cases}$$

where $K^{-1} = \{k^{-1} \mid k \in K\}$. A set M of messages is called closed, if for any $m \in M$ there exists $M' \in wc(m)$ such that $M' \subseteq M$.

Example 4.2 *Consider the message $m = (\{A, N\}_k, B)$. Then $wc(m)$ consists of the following sets:*

$K^{-1} \cup \{(\{A, N\}_k, B), \{A, N\}_k, (A, N), A\}$ $\quad$ $K^{-1} \cup \{(\{A, N\}_k, B), \{A, N\}_k, k\}$

$K^{-1} \cup \{(\{A, N\}_k, B), \{A, N\}_k, (A, N), N\}$ $\quad$ $K^{-1} \cup \{(\{A, N\}_k, B), B\}$.

We can prove the following:

Lemma 4.1 *Let S be a closed set of messages. And let E be a set of messages such that $S \cap E = \emptyset$. Then, $E \not\vdash_c S$. In other words, if S is closed then no message in S can be derived uniquely by the composition rules.*

We use the notation $E\langle w_i, S_i\rangle_I$ for $\bigwedge_{i\in I} E\langle w_i\rangle S_i$. Our purpose now is to define conditions on w_i and S_i such that for any set E of messages, if $E\langle w_i, S_i\rangle_I$ then $m\langle w_i, S_i\rangle_I$, for any message m derivable from E. In other words, such conditions ensure that $E\langle w_i, S_i\rangle_I$ is stable under the derivations rules defining the intruder. Remember that closure guarantees stability only under composition rules.

Example 4.3 *Let $E = \{s_1, s_2\}$ be a set of messages. Then we have $E\langle w\rangle(s_1, s_2)$. But we have both $E \vdash (s_1, s_2)$ and $\neg(s_1, s_2)\langle w\rangle(s_1, s_2)$.*

This example shows that we need to consider only closed sets of secrets. But this is not sufficient, as showed by the following example.

Example 4.4 *Let $E = \{\{\{s\}_{k_1}, k_2\}$ be a set of messages. We have $E\langle(\{\{s\}_{k_1}\}_{k_2}, 11)\rangle s$. But we have both $E \vdash \{\{s\}_{k_1}\}_{k_2}$ and $\neg\{\{s\}_{k_1}\}_{k_2}\langle(\{\{s\}_{k_1}\}_{k_2}, 11)\rangle s$.*

Hence, we need to deal also with the interior term transducers. To do so, let (b, p) be a term transducer. Then, we denote by $\mathrm{lpt}(b, p)$ the next term transducer in b from above that dominates $b_{|p}$, if it exists. A formal definition is given in Appendix A.1 but let us give an example.

Example 4.5 *Let b be the term $\{(\{N\}_{k'}, A)\}_k$ with $k, k' \in K$. Then, $lpt(b, 111) = (\{N\}_{k'}, 1)$. But $lpt(b, 12)$ does not exist neither $lpt(b, 11)$ does.*

We have now everything we need to express the conditions that guarantee stability under the intruder's derivations:

Definition 4.3 *$(w_i, S_i)_{i\in I}$ is called* well-formed*, if the following conditions are satisfied for every $i \in I$:*

- *S_i is closed,*
- *if $w_i = (b, r).w$ and if there exists a term transducer $(b_1, r_1) = lpt(b, r)$, then there exists $j \in I$ such that one of the following is true:*
  - *$b \in S_j$*
  - *$w_j = (b_1, r_1).w$ and $S_i \subseteq S_j$.*

The main property of $E\langle w_i, S_i\rangle_I$ is that it is stable under the intruder's deduction rules. Indeed, we have:

Proposition 4.1 *Let E be a set of messages such that $E\langle w_i, S_i\rangle_I$ and let $(w_i, S_i)_{i\in I}$ be well-formed. Moreover, let m be a message with $E \vdash m$. Then, $m\langle w_i, S_i\rangle_I$.*

Proof See Appendix A.2. □

The modality $E\langle w\rangle S$ has another interesting property with respect to intruder's derivations:

Proposition 4.2 *Let m be a message and E a set of messages such that $\mathcal{K} \setminus K^{-1} \subseteq E$. Then, $E \nvdash m$ iff there exists a set of messages $A \in wc(m)$ s.t. $E\langle\epsilon\rangle A$.*

Proof See Appendix A.3. □

4.2 TSPL: A Logic for Security Properties

The syntax of TSPL is defined in Table 1, where X is a fixed second-order variable that ranges over sets of messages and x is a meta-variable that ranges over the set $\mathcal{V}$ of first-order variables. First-order variables range over messages; t is a meta-variable over terms. Moreover, S is a finite set of terms and w is a finite sequence of term transducers that can contain free variables. The formulae are interpreted over a restricted set of configurations $\mathcal{C}onf = \{(\sigma, E, \nu, l) | (\sigma, E, \nu, l) \in \mathcal{C}onf, \mathcal{K} \setminus K^{-1} \subseteq E\}$.

$\Psi ::=$	$\top \mid \sum_{i=1}^{n} a_i c_i + \sum_{j=1}^{m} b_j T_j \bowtie \delta \mid \Psi_1 \wedge \Psi_2 \mid \Psi_1 \vee \Psi_2$	time constraint formulae
$\Phi ::=$	$X\langle w\rangle S \mid x\langle w\rangle S \mid x = t \mid pc = \ell \mid \top \mid \bot \mid \Phi \wedge \Phi \mid \neg\Phi$	term formulae
$\Gamma ::=$	$\Phi \mid \Psi \mid \Gamma \vee \Gamma \mid \Gamma \wedge \Gamma$	TSPL formulae

Table 1: The set of formulae TSPL.

Notice that omitting the negation for time constraints is not essential as any negation of a time constraint can be put in a positive form.

Definition 4.4 (semantics) *The semantics of* TSPL *is defined by the following clauses:*

- $[\![\Psi]\!] = \{(\sigma, E, \nu, \ell) \mid [\![\Psi]\!]_{\nu,\sigma} = 1\}$
- $[\![X\langle w\rangle S]\!] = \{(\sigma, E, \nu, \ell) \mid E\sigma\langle w\sigma\rangle S\sigma\}$
- $[\![x\langle w\rangle S]\!] = \{(\sigma, E, \nu, \ell) \mid \{\sigma(x)\}\langle w\sigma\rangle S\sigma\}$
- $[\![x = t]\!] = \{(\sigma, E, \nu, \ell) \mid \sigma(x) = \sigma(t)\}$.

- $[\![pc = \ell]\!] = \{(\sigma, E, \nu, \ell) \mid (\sigma, E, \nu, \ell) \text{ is a configuration}\}$
- $[\![\neg\varphi]\!] = \mathcal{C}onf \setminus [\![\varphi]\!]$
- $[\![\top]\!] = \mathcal{C}onf$
- $[\![\bot]\!] = \emptyset$
- $[\![\Gamma_1 \wedge \Gamma_2]\!] = [\![\Gamma_1]\!] \cap [\![\Gamma_2]\!]$
- $[\![\Gamma_1 \vee \Gamma_2]\!] = [\![\Gamma_1]\!] \cup [\![\Gamma_2]\!]$

For convenience of notations, we extend the set of formulae TSPL as follows:

$$\text{TSPL}_+ \ni \varphi, \psi ::= \ldots \mid (X, x)\langle w\rangle S \mid t\langle w\rangle S$$

The semantics of the newly introduced formulae is:

$$[\![t\langle w\rangle S]\!] = \{(\sigma, E, \nu, \ell) \mid t\sigma\langle w\sigma\rangle S\sigma\}$$

$$[\![(X, x)\langle w\rangle S]\!] = [\![X\langle w\rangle S]\!] \cap [\![x\langle w\rangle S]\!]$$

We can prove that any formulae of the form $t\langle w\rangle S$ is definable in TSPL. We use the notations $(\sigma, E, \nu, \ell) \models \varphi$ for $(\sigma, E, \nu, \ell) \in [\![\varphi]\!]$, $t\langle\not w\rangle S$ for $\neg t\langle w\rangle S$, $X\langle\not w\rangle S$ for $\neg X\langle w\rangle S$, and $(X, t)\langle\not w\rangle S$ for the formula obtained from $t\langle\not w\rangle S$ by replacing any occurrence of $y\langle\not w\rangle S$ by $(X, y)\langle\not w\rangle S$ for all variables y. Also, given s a term, we write $X\langle w\rangle s$ instead of $X\langle w\rangle\{s\}$ and $t\langle w\rangle s$ instead of $t\langle w\rangle\{s\}$. We identify formulae modulo the usual properties of boolean connectives such as associativity and commutativity of $\wedge$, $\vee$, distributivity etc... and use $\Rightarrow$ as the classical logical implication (it can be easily defined in TSPL logic using set inclusion). Also, for any formula Φ, we denote by $fn(\Phi)$ the formula obtained from Φ by pushing "inside" the negation $\neg$ as much as possible (using distributivity of $\neg$ w.r.t. to $\wedge$ and $\vee$).

Well-formed formulae. In Definition 4.3, we introduced when $(w_i, S_i)_{i\in I}$ is well-formed. As now we are dealing with formulae, we have to define when a formula is well-formed in the same sense.

Definition 4.5 *A formula Φ is* well-formed, *if for any sequence of term transducers w and closed set of terms S, whenever $\Phi \Rightarrow X\langle w\rangle S$, there exist $(w_i, S_i)_{i\in I}$ well-formed, such that $\Phi \Rightarrow \bigwedge_{i\in I} X\langle w_i\rangle S_i$ and $(w, S) \in (w_i, S_i)_{i\in I}$.*

The main property satisfied by well-formed formulae is an a parallel to Proposition 4.1 and given by the following corollary, which is a direct consequence of Definitions 4.3 and 4.5.

Corollary 4.1 *Let Φ be a well-formed formula such that $\Phi \Rightarrow X\langle w\rangle S$ and let $(\sigma, E, l) \in [\![\Phi]\!]$. If m is a message such that $E\sigma \vdash m$, then $m\langle w\sigma\rangle S\sigma$.*

Now, the property of Corollary 4.1 turns out to be crucial for developing a complete weakest precondition calculus and well-formedness has to be preserved. Therefore, we introduce the function $\mathcal{H}$. It takes as arguments a formula $X\langle b.w\rangle S$ and computes the weakest (the largest w.r.t. set inclusion) well-formed formula $\mathcal{H}(X\langle b.w\rangle S)$, such that $\mathcal{H}(X\langle b.w\rangle S) \Rightarrow X\langle b.w\rangle S$:

$$\mathcal{H}(X\langle b.w\rangle S) = \begin{cases} X\langle b.w\rangle S & \text{if } \mathrm{lpt}(b) \text{ is undefined} \\ X\langle b.w\rangle S \wedge & \\ \left(\mathcal{H}(X\langle b_1.w\rangle S) \vee \bigvee_{S'\in wc(t)} X\langle\epsilon\rangle S'\right) & \text{if } b = (t, p) \wedge b_1 = \mathrm{lpt}(b) \end{cases}$$

Proposition 4.3 *Let Φ be a well-formed formula. Let $b.w$ be a sequence of term transducers and S a closed set of terms such that $\Phi \Rightarrow X\langle b.w\rangle S$. Then $\Phi \Rightarrow \mathcal{H}(X\langle b.w\rangle S)$.*

Proof A direct consequence of Definitions 4.3 and 4.5. □

5 Computing Predecessors

We are interested in proving reachability properties of bounded timed cryptographic protocols. Given a property φ and an action α, $pre(\alpha, \mathcal{C})$ denotes the smallest set of configurations that by executing α may lead to a configuration that satisfies φ. That is,

Definition 5.1 (predecessors) *The predecessor of a set of configurations $\mathcal{C} \subseteq \mathcal{C}onf$ with respect to an action α, denoted $pre(\alpha, \mathcal{C})$ is the set of configurations s, such that there is at least one possible execution of α that leads from s to a configuration in $\mathcal{C}$. More precisely*

$$pre(\alpha, \mathcal{C}) ::= \big\{(\sigma, E, \nu, l) \mid \exists (\sigma', E', \nu', l') \in \mathcal{C} \text{ s. t. } (\sigma, E, \nu, l) \xrightarrow{\alpha} (\sigma', E', \nu', l')\big\}.$$

Given a formula Φ, we use $pre(\alpha, \Phi)$ instead of $pre(\alpha, [\![\Phi]\!])$ to denote the predecessor of a formula $\Phi \in$ TSPL.

The purpose of this section is to show that $pre(\alpha, \Phi)$ is effectively expressible in TSPL, when Φ is a positive boolean combination of time constraints and term formulae of the form:

$$x = t \mid pc = \ell \mid \top \mid \bot \mid x \neq t \mid pc \neq \ell \mid X\langle \not w \rangle S \mid x\langle \not w \rangle S.$$

First, it is easy to see that $pre(\alpha, \Phi) = \Phi$, if α is a time passing action and Φ is a term formula. Also, for any action $\alpha = l \xrightarrow{g, \mathcal{R}, !t} l'$, respectively $\alpha = l \xrightarrow{g, \mathcal{R}, ?t} l'$, and any time constraint Ψ, we have $pre(\alpha, \Psi) = g \wedge pc = \ell \wedge \Psi[R]$.

Moreover, it can easily be shown that for the actions considered here *pre* distributes with respect to disjunction; in addition, if α is an output or an input, we can easily prove that *pre* distributes with conjunction too.

5.1 Time passing and time constraints

In this section, we show that the predecessor of $[\![\Psi]\!]$, where Ψ is a time constraint, can be described by an TSPL formula. We consider the action $\xrightarrow{\tau}$, i.e. time passing. The case of input and output actions is described above.

We need first to define three kinds of normal forms for time constraints. Let Ψ be the atomic time constraint $\sum_{i=1}^{n} a_i c_i + \sum_{j=1}^{m} b_j T_j \bowtie d$. We denote by $\mathscr{C}(\Psi)$ the sum of the coefficients of clocks, i.e. $\sum_{i=1}^{n} a_i$. Then, an atomic time constraint $\Psi \equiv \sum_{i=1}^{n} a_i c_i + \sum_{j=1}^{m} b_j T_j \bowtie d$ is in *positive normal form* (PNF for short), if $\mathscr{C}(\Psi) > 0$; it is in *negative normal form* (NNF for short), if $\mathscr{C}(\Psi) < 0$; and finally, it is in *0-normal form*, if $\mathscr{C}(\Psi) = 0$.

Clearly any time constraint can be put in the form of a disjunction of conjunctions of the form $\Psi_1 \wedge \Psi_2 \wedge \Psi_3$, where Ψ_1 is a conjunction of formulae in PNF, Ψ_2 is a conjunction of formulae in NNF and Ψ_3 is a conjunction of formulae in 0-NF. For the rest of this section, we write $\psi \in \Psi_i$ to state that ψ is a conjunct of Ψ_i, i.e., we view conjunctions of formulae as sets of formulae.

Thus, let us consider a time constraint of the form $\Psi_1 \wedge \Psi_2 \wedge \Psi_3$ as above. Then, $pre(\xrightarrow{\tau}, \Psi_1 \wedge \Psi_2 \wedge \Psi_3)$ can be described by the formula $\exists \delta \geq 0 \cdot \Psi_1 + \delta \wedge \Psi_2 + \delta \wedge \Psi_3 + \delta$. We have then to show that we can eliminate the quantification on δ while obtaining a time constraint.

First, notice that $\Psi_3 + \delta$ is logically equivalent to Ψ_3, since it is in 0-NF. Therefore, we can rewrite the formula to the equivalent formula $\exists \delta \geq 0 \cdot (\Psi_1 + \delta \wedge \Psi_2 + \delta) \wedge \Psi_3$ and focus on discussing how to transform $\exists \delta \geq 0 \cdot (\Psi_1 + \delta \wedge \Psi_2 + \delta)$ into an equivalent time constraint. Let us explain the main idea by considering the simple case where Ψ_1 and Ψ_2 are simple conjunctions.

The simple case Consider a PNF time constraint $\Psi_1 \equiv \sum_{i=1}^{n} a_i c_i + \sum_{j=1}^{m} b_j T_j \bowtie_1 d$ and a NNF $\Psi_2 \equiv \sum_{i=1}^{n} a'_i c_i + \sum_{j=1}^{m} b'_j T_j \bowtie_2 d'$. Then, we have:

$$\begin{array}{l} \Psi_1 + \delta \equiv \sum_{i=1}^{n} a_i c_i + \sum_{j=1}^{m} b_j T_j + \delta \sum_{i=1}^{n} a_i \bowtie_1 d \\ \Psi_2 + \delta \equiv \sum_{i=1}^{n} a'_i c_i + \sum_{j=1}^{m} b'_j T_j + \delta \sum_{i=1}^{n} a'_i \bowtie_2 d' \end{array}$$

By multiplying with $\mathscr{C}(\Psi_1)$ and $|\mathscr{C}(\Psi_2)|$ we have:

$$\Psi_1 + \delta \equiv \sum_{i=1}^{n} |\mathscr{C}(\Psi_2)| a_i c_i + \sum_{j=1}^{m} |\mathscr{C}(\Psi_2)| b_j T_j + \delta |\mathscr{C}(\Psi_2)| \sum_{i=1}^{n} a_i \bowtie_1 |\mathscr{C}(\Psi_2)| d$$
$$\Psi_2 + \delta \equiv \sum_{i=1}^{n} \mathscr{C}(\Psi_1) a'_i c_i + \mathscr{C}(\Psi_1) \sum_{j=1}^{m} b'_j T_j + \delta \mathscr{C}(\Psi_1) \sum_{i=1}^{n} a'_i \bowtie_2 \mathscr{C}(\Psi_1) d'$$

Adding the right-hands of the equivalences yields the time constraint:

$$\sum_{i=1}^{n} a''_i c_i + \sum_{j=1}^{m} b''_j T_j \bowtie' |\mathscr{C}(\Psi_2)| d + \mathscr{C}(\Psi_1) d'$$

with $a''_i = |\mathscr{C}(\Psi_2)| a_i + \mathscr{C}(\Psi_1) a'_i$, $b''_j = |\mathscr{C}(\Psi_2)| b_i + \mathscr{C}(\Psi_1) b'_i$ and if $\bowtie_1 \equiv \bowtie_2$ then $\bowtie' \equiv \bowtie_1$ else $\bowtie' \equiv <$.

Let us denote this formula by $\Delta(\Psi_1, \Psi_2)$. Notice that $\Delta(\Psi_1, \Psi_2)$ is independent of δ. One can prove that $\exists \delta \geq 0 \cdot (\Psi_1 + \delta \wedge \Psi_2 + \delta)$ is equivalent to the time constraint $\Psi_1 \wedge \Delta(\Psi_1, \Psi_2)$. The conjunct Ψ_1 has to be kept as we are interesting in the predecessors, thus the upper bound on the clocks must be satisfied as time only increases.

The general case Let us now return to the general case, where Ψ_1 and Ψ_2 are arbitrary conjunctions of formulae in PNF, respectively, NNF. To handle this case we generalize Δ to sets (conjunctions of formulae as follows):

- $\Delta(\emptyset, \psi) = \top$.
- $\Delta(\psi, \emptyset) = \psi$.
- $\Delta(\Psi_1, \Psi_2) = \bigwedge_{\psi_1 \in \Psi_1, \psi_2 \in \Psi_2} \Delta(\psi_1, \psi_2)$

Then we can prove that $\exists \delta \geq 0 \cdot (\Psi_1 + \delta \wedge \Psi_2 + \delta)$ is equivalent to $\Delta(\Psi_1, \Psi_2)$.

Summarizing together, we can transform $\exists \delta \geq 0 \cdot \Psi_1 + \delta \wedge \Psi_2 + \delta \wedge \Psi_3 + \delta$ into the equivalent time constraint $\Delta(\Psi_1, \Psi_2) \wedge \Psi_1 \wedge \Psi_3$. Hence, if we define $\mathbf{Pre}(\xrightarrow{\tau}, \Psi_1 \wedge \Psi_2 \wedge \Psi_3) \stackrel{def}{=} \Delta(\Psi_1, \Psi_2) \wedge \Psi_1 \wedge \Psi_3$, we obtain the following result:

Proposition 5.1 *For any time constraint Ψ,*

$$pre(\xrightarrow{\tau}, [\![\Psi]\!]) = [\![\mathbf{Pre}(\xrightarrow{\tau}, \Psi)]\!].$$

5.2 Output action and atomic term formulae

Throughout this section let $\alpha = l \xrightarrow{g, \mathcal{R}, !t} l'$, and let $\tilde{c}$ be all the clocks that occur in t and do not occur in $\mathcal{R}$. We show that we can express $pre(\alpha, \varphi)$, for any atomic term formula φ. The core point here is how we deal with the clocks occurrences in the sent message. Since the values of clocks change with time, we have to freeze these values in the message added to the intruder knowledge; we do this by replacing in t, all occurrences of clocks that are not reseted $\tilde{c}$ with fresh time variables $\tilde{T}_c$ and by introducing the constraints $\tilde{T}_c = \tilde{c}$. For more details, see *Example A.1*, presented in Appendix A.8.

Let us define $\mathbf{Pre}(\alpha, \varphi)$:

1. $\mathbf{Pre}(\alpha, \varphi) \stackrel{def}{=} g \wedge pc = \ell \wedge (\varphi \vee ((X, t[0/\mathcal{R}, \tilde{T}_c/\tilde{c}]) \langle\!\not\vdash\!\rangle S \wedge \tilde{T}_c = \tilde{c}))$, where $\tilde{T}_c$ are fresh time variables, if φ is a formula of the form $X \langle\!\not\vdash\!\rangle S$ or $(X, x) \langle\!\not\vdash\!\rangle S$.
2. $\mathbf{Pre}(\alpha, \varphi) \stackrel{def}{=} g \wedge pc = \ell \wedge \varphi$, if φ is of the form $x \neq t'$, $x = t'$, $\top$ or $\bot$.

Then, we have the following :

Proposition 5.2 *For any output action α and atomic term formula φ,*

$$pre(\alpha, [\![\varphi]\!]) = [\![\mathbf{Pre}(\alpha, \varphi)]\!].$$

5.3 Input action and atomic term formulae

Throughout this section let $\alpha = l \xrightarrow{g,\mathcal{R},?t(\tilde{x})} l'$. We show that we can express $pre(\alpha, \varphi)$, for any atomic term formula φ. To do so, we need to introduce a few definitions and prove a few intermediate results.

Let t be a term and p a critical position in t. Then, we denote by $\mathrm{lpp}(t, p)$ recursively on the structure of t as follows:

- if t is a constant or a variable then $\mathrm{lpp}(t, p)$ is undefined.
- if $t = (t_1, t_2)$ and $p = 1 \cdot p'$ then $\mathrm{lpp}(t, p) = 1 \cdot \mathrm{lpp}(t_1, p')$. Similarly, when $p = 2 \cdot p'$.
- if $t = \{t'\}_k$ and $k \in K$ then $\mathrm{lpp}(t, p) = \epsilon$.
- if $t = \{t'\}_k$ and $k \notin K$ then $\mathrm{lpp}(t, p) = 1 \cdot \mathrm{lpp}(t', 1^{-1}p)$.

Example 5.1 *Consider the term $t = (\{A, \{N\}_{k_1}\}_{k_2}, N)$, where $k_1, k_2 \in K$. Let $p = 1121$ and $p' = 2$. Thus, $t_{|p} = t_{|p'} = N$. Then, we have $lpp(t, p) = 1$, which corresponds to the key k_2; $lpp(t, p')$ is, however, undefined.*

Given a term t, let $F(t)$ denote the formula $\bigwedge_{S' \in wc(t)} X\langle \not\in \rangle S'$. The intuitive explanation of next lemma is the following: being in a state (σ, E, ν, l), in order to be able to make an input $t(\tilde{x})$, such that $\tilde{x}$ are instantiated by ρ, it must be that $(\sigma, E, \nu, l) \in [\![F(t\rho)]\!]$.

Lemma 5.1 *Let E be a set of terms, l be a label, ν be a clocks valuation and let ρ and σ be ground substitutions such that $dom(\rho) = \tilde{x}$ and $(dom(\sigma) \cup var(E)) \cap \tilde{x} = \emptyset$. Then it holds $(\sigma, E, \nu, l) \in [\![F(t\rho)]\!]$ iff $E\sigma \vdash t(\sigma \oplus \rho)$.*

Proof See Appendix A.5. □

First, notice that the effect of an input action $?t$ depends on the messages that match with t and that are known by the intruder. Therefore, we need to characterize the set of configurations s, such that if in the next step x is instantiated by an input $?t(\tilde{x})$, the reached configuration s' satisfies $x\langle \not\in \rangle S$.

To understand how this characterization is obtained, the best is to consider the negation of $x\langle \not\in \rangle S$, i.e., $x\langle w \rangle S$. The key idea can be explained by considering the sequence of actions $?t(\tilde{x}); !x$. That is, if a secret s that appears in x has to be protected then it has to appear in x under an encryption. Thus, before executing $?t(\tilde{x}); !x$, it should be the case that if we provide the intruder with the term transducer that takes as input $t(\tilde{x})$ and yields x, it is not possible to derive s.

Lemma 5.2 *Let t be a term, S a set of terms, w a sequence of term transducers, x a variable and $P_{x,t}$ the set of critical positions of x in t. Let*

$$\mathcal{K}(t, x, w, S) = X\langle w \rangle S \wedge \bigwedge_{p = lpp(t, p_x), p_x \in P_{x,t}} \mathcal{H}(X\langle (t|_p, p^{-1}p_x).w \rangle S).$$

Let E be a set of terms, l and l' labels, and ρ, σ ground substitutions such that $dom(\rho) = \tilde{x}$, $x \in \tilde{x}$, $(dom(\sigma) \cup var(E)) \cap \tilde{x} = \emptyset$. Let Φ a well-formed formula such that whenever $E\sigma \vdash t(\sigma \oplus \rho)$, it holds

$$(\sigma \oplus \rho, E, l') \in [\![(X, x)\langle w \rangle S]\!] \text{ iff } (\sigma, E, l) \in [\![\Phi]\!].$$

Then $[\![\Phi]\!] = [\![\rho(\mathcal{K}(t, x, w, S))]\!]$.

Proof See Appendix A.6. □

Let now α be the action $\alpha = l \xrightarrow{g,\mathcal{R},?t(\tilde{x})} l'$, where $\tilde{x}$ the variables that are instantiated by this action. We then define $\mathbf{Pre}(\alpha, \varphi)$ as follows:

1. $\mathbf{Pre}(\alpha, \varphi) \stackrel{def}{=} g \wedge pc = \ell \wedge F(t) \wedge \varphi$, if φ is of the form $X\langle \not\in \rangle S$. $(X, y)\langle \not\in \rangle S$, $x \neq t'$, $x = t'$,$\top$ or $\bot$ and $y \notin \tilde{x}$.
2. $\mathbf{Pre}(\alpha, (X, x)\langle \not\in \rangle S) \stackrel{def}{=} g \wedge pc = \ell \wedge F(t) \wedge \neg\mathcal{K}(t, x, w, S)$, if $x \in \tilde{x}$.

Proposition 5.3 *For any input action α and atomic term formula φ,*

$$pre(\alpha, [\![\varphi]\!]) = [\![\mathbf{Pre}(\alpha, \varphi)]\!].$$

5.4 Collecting the results together

It is easy to see that for any formula $\varphi \in$ TSPL and any action α, $\mathbf{Pre}(\alpha, \varphi) \in$ TSPL. Then, we have the following theorem:

Theorem 5.1 *Let α be any action and φ any formula in* TSPL. *Then,*

$$pre(\alpha, [\![\varphi]\!]) = [\![\mathbf{Pre}(\alpha, \varphi)]\!].$$

6 Decidability of TSPL

In this section, we prove decidability of the existence of a model of an TSPL formula. Notice that since we showed in Section 5 that given a formula φ in TSPL and a bounded CP π, one can compute $\mathbf{Pre}(\pi, \varphi)$, decidability of the satisfiability of formulae yields a decision procedure for reachability of configurations described by TSPL formulae.

To prove decidability for the satisfiability of TSPL formulae we follow a rule based approach (e.g., [JK91, Com91] for two nice surveys) i.e.:

1. We introduce a set of formulae in *solved form*. For these formulae it is easy to decide whether a model exists.
2. We introduce a set of rewriting rules to transform any formula in the existential fragment into a solved form.
3. We prove soundness and completeness of these rules.
4. We also prove their termination for a given control, i.e. that normal forms are reached and that normal forms are indeed in solved form.

We will encounter two sorts of rewriting rules:

- Deterministic rules are of the form $\varphi \rightarrow \varphi'$. They transform a given problem into a single problem. A deterministic rule is sound, if $[\![\varphi]\!] = [\![\varphi']\!]$.
- Non-deterministic rules of the form $\varphi \rightarrow \varphi_1, \cdots, \varphi_n$. They transform a given problem into a set of problems. A non-deterministic rule is sound, if $[\![\varphi]\!] = \bigcup_{i=1}^{n} [\![\varphi_i]\!]$.

In this section, we do not consider formulae of the from $pc = \ell$. It will be clear that adding these formulae does not add any technical difficulty; it is only cumbersome to consider them here. Moreover, it is obvious that as we consider satisfiability we can restrict ourselves to conjunctions of literals.

Let φ be a *conjunction* of literals, i.e.,

$$X\langle w\rangle S \mid x\langle w\rangle S \mid x = t \mid \top \mid X\langle \not w\rangle S \mid x\langle \not w\rangle S \mid x \neq t \mid \bot \mid \sum_{i=1}^{n} a_i c_i + \sum_{j=1}^{m} b_j T_j \bowtie d$$

6.0.1 Solved form

A formula is called in solved form if is syntactically equal to $\top$, $\bot$ or to a conjunction $\Psi \wedge \varphi$ where Ψ is a time constraint and φ is of the form:

$$\bigwedge_{i=1}^{n} [\bigwedge_{j=1}^{m_i} x_i\langle \epsilon\rangle t_i^j \wedge \bigwedge_{j=1}^{l_i} x_i\langle \not\epsilon\rangle u_i^j \wedge \bigwedge_{j=1}^{o_i} x_i \neq v_i^j]$$

such that:

- For any $i = 1, \cdots, n$, $x_i \notin var(t_i^j)$, $x_i \notin var(u_i^j)$, and $x_i \notin var(v_i^j)$.

- There is an ordering $x_{i_1}, \cdots, x_{i_n}$ of $x_1, \cdots, x_n$ such that $\bigcup_{k=1}^{l_{i_k}} var(u_{i_k}^k) \cap \{x_{i_{k+1}}, \cdots, x_{i_n}\} = \emptyset$.

We now show how one can check whether a formula in solved form has a model. We only consider the third type of solved formulae. To begin with let us first assume that the time constraint is $\top$, that is, we only have to deal with φ. We will later show how to reduce the general case to this one.

Satisfiability of φ So, let φ a conjunction as above. We consider clocks and time variables as constant symbols and define a particular substitution σ such that φ has a model iff it is satisfied by σ. To do so, let $k \in K$ be a fixed key. Let $F(n)$, for $n \geq 1$, denote n concatenations of k, i.e., $F(1) = k$ and $F(n+1) = \mathbf{pair}(k, F(n))$. Let now N be a natural number strictly bigger than the size of the formula φ. We then define the substitution σ recursively as follows:

- If $n = 1$, i.e., there is only one variable then $\sigma(x_{i_1}) = (u_{i_1}^1, (\cdots, (u_{i_1}^{l_{i_1}}, \{F(N+i_1)\}_k) \cdots))$. In case $l_{i_1} = 0$ this term is understood as $\{F(N+i_1)\}_k$.
- If $n > 1$ then replace x_{i_1} by $\sigma(x_{i_1})$ in φ. This yields a new formula φ' and the ordering $x_{i_2}, \cdots, x_{i_n}$, and by recursion, a substitution σ'. Then, let

$$\sigma = [x_{i_1} \mapsto (u_{i_1}^1, (\cdots, (u_{i_1}^{l_{i_1}}, \{F(N+i_1))\}_k) \cdots))] \oplus \sigma'.$$

Theorem 6.1 *Let φ be a term formula in solved form syntactically different from $\top$ and $\bot$. Let σ be the substitution as defined above. Then, φ has a model iff σ satisfies φ.*

> **Proof** We only give a sketchy idea of the main argument why the Theorem holds. The interesting implication to prove is the following: If σ does not satisfy φ then φ has no model.
>
> Now, since σ has been defined such that $\sigma(x)$ is not a sub-term of φ, for any $x = x_1, \cdots, x_n$, we have the two crucial properties: 1.) If $u\sigma\langle\not\in\rangle t\sigma$ then $u\langle\not\in\rangle t$ and 2.) If $u\sigma \neq t\sigma$ then $u \neq t$. On the other hand, we can prove if σ is not a model of φ then $u_i^j\sigma\langle\not\in\rangle t_i^q\sigma$, for some $i \in \{1, \cdots, n\}$, $j \in \{1, \cdots, l_i\}$ and $q \in \{1, \cdots, m_i\}$. Therefore, $u_i^j\langle\not\in\rangle t_i^q$, and hence, φ has no model. □

The general case Let us now return to the case where Ψ is a conjunction of time constraints. It turns out that only the equalities between the variables in $\mathcal{C} \cup \mathcal{Y}$ that are implied by Ψ might rule out some of the models of φ. That is, we need only to take into account such equalities. Let us illustrate this by an example. Consider the formula $\varphi' \equiv x\langle\epsilon\rangle(A, c) \wedge x\langle\not\in\rangle(A, T)$. Then, $\varphi' \wedge 0 \leq c \leq 1 \wedge 0 \leq T \leq 1$ is satisfiable; while $\varphi' \wedge c - T = 0$ is not. Indeed, in the first the time constraint does not imply any equality; while in the second case it implies $c = T$.

Therefor, we proceed as follows: We compute the strongest time constraint Ψ' of the form $\bot$ or

$$\bigwedge_{i=1}^{m} z_i = z_i'$$

where $z_i, z_i' \in \mathcal{C} \cup \mathcal{Y}$ and such that Ψ implies Ψ' and $\{z_i \mid i = 1, \cdots, n\} \cap \{z_i' \mid i = 1, \cdots, n\} = \emptyset$.

If Ψ' is $\bot$ then $\Psi \wedge \varphi$ is not satisfiable otherwise we replace in φ each z_i by z_i' and check that the obtained formula is satisfiable using the substitution defined above.

6.0.2 Rewriting rules

Theorem 6.2 *Application of the rules of Table 7 terminates in a solved form.*

> **Proof** See Appendix A.9. In Table 7 we use the notation $\mathcal{J}(t, w, s)$ which denotes a TSPL formula equivalent to $t\langle w\rangle s$. The definition and the equivalence of this formula are given in the appendix. □

$x = x \mapsto \top$	$t\langle w\rangle t \mapsto \bot$	$\bot \wedge \Phi \mapsto \bot$	$t \neq t \mapsto \bot$	$t\langle \not w\rangle t \mapsto \top$	$\top \wedge \Phi \mapsto \Phi$
$x = t \mapsto \bot$	if $x \in \mathcal{V}ar(t) \wedge x \not\sqsubseteq_s t$		$w\langle \epsilon\rangle t \mapsto \top$	if $x \in \mathcal{V}ar(t) \wedge x \not\sqsubseteq_s t$	
$x \neq t \mapsto \top$	if $x \in \mathcal{V}ar(t) \wedge x \not\sqsubseteq_s t$		$w\langle \not\epsilon\rangle t \mapsto \bot$	if $x \in \mathcal{V}ar(t) \wedge x \not\sqsubseteq_s t$	

Table 2: Eliminate trivial sub-formulae

$$x = t \wedge \Phi \quad \mapsto \quad \Phi[t/x] \quad \text{if } x \notin \mathcal{V}ar(t)$$

Table 3: Replacement

$t\langle w\rangle s$	$\mapsto$	$\mathcal{J}(t, w, s)$, if $t \notin \mathcal{X} \cup \mathcal{C} \cup \mathcal{T} \cup \mathbb{R}_{\geq 0}$	**D1.1**
$t\langle w\rangle s$	$\mapsto$	$t \neq s$, if $t \in \mathcal{C} \cup \mathcal{T} \cup \mathbb{R}_{\geq 0}$	**D1.2**
$x\langle (b, p).w\rangle s$	$\mapsto$	$x\langle \epsilon\rangle s \wedge x\langle \epsilon\rangle b,\ x\langle \epsilon\rangle s \wedge b|_p\langle w\rangle s$	**D2**
$s = t$	$\mapsto$	$\mu(s, t)$ if $s, t \notin \mathcal{X} \cup \mathcal{C} \cup \mathcal{T} \cup \mathbb{R}_{\geq 0}$	**D3**

Table 4: Decompose

$$\bigwedge_{i \in I} X\langle w_i\rangle s_i \wedge \bigwedge_{j \in J} X\langle \not w_j\rangle s'_j \mapsto \bigwedge_{j \in J} \Big[\bigwedge_{i \in I} z_j\langle w_i\rangle s_i \wedge z_j\langle \not w_j\rangle s'_j \Big]$$

where z_j with $j \in J$ are new variables

Table 5: Elimination X

$$\varphi \mapsto \varphi[y/x]$$

if x and y are syntactically different and $x \leq y$ and $y \leq x$, where $\leq$ is the reflexive transitive closure of $<$ with "$x < y$ iff there there is a sub-formula of φ of the form $y\langle \not w\rangle t$ with $x \in var(t)$".

Table 6: Occur-check

Table 7: Rules for transformations into a solved form

7 Conclusions

In this paper, we have proved the decidability of a large class of reachability properties, including secrecy and authentication, for **timed** bounded protocols. Our model for specifying timed protocols uses clocks, time variables and time-stamps. This work can be extended in several ways:

1. our model can be naturally extended to associate time values to short term keys such that if the intruder obtains a message encrypted by a short term key then after the specified amount of time elapses the key becomes known by the intruder. Our model and verification method can be extended to handle this model.

2. our model can also be extended handle drifting clocks. It is well-known that models with clocks with drifts in bounded intervals can be transformed into models with perfect clocks modulo an abstraction, that is, taking into account more behavior. As discussed by Gong [Gon92] drifting clocks can add subtle attacks.

3. in the full version of this paper we show how we can use our logic to device an abstract interpretation based method for unbounded protocols.

References

[AD94] R. Alur and D. Dill. A Theory of Timed Automata. *Theoretical Computer Science*, 126, 1994.

[AFH91] R. Alur, T. Feder, and T.A. Henzinger. The benefits of relaxing punctuality. In *Proceedings of the 10th ACM Symposium on Principles of Distributed Computing*, pages 139–152. ACM Press, 1991.

[AL00] R. M. Amadio and D. Lugiez. On the reachability problem in cryptographic protocols. In *International Conference on Concurrency Theory*, volume 1877 of *LNCS*, pages 380–394, 2000.

[BL95] A. Bouajjani and Y. Lakhnech. Temporal logic + timed automata: expressiveness and decidability. In I. Lee and S. A. Smolka, editors, *CONCUR'95: Concurrency Theory*, volume 962 of *LNCS*, pages 531–546. Springer-Verlag, 1995.

[Bor01] M. Boreale. Symbolic trace analysis of cryptographic protocols. In *ICALP: Annual International Colloquium on Automata, Languages and Programming*, 2001.

[BP98] G. Bella and L. C. Paulson. Machanising BAN Kerberos by the inductive method. In A. J. Hu and M. Y. Vardi, editors, *Proceedings of the 10th International Conference on Computer-Aided Verification (CAV'98)*, pages 416–427, Vancouver, B.C., Canada, June 1998. Springer-Verlag LNCS 1427.

[CJ97] J. Clark and J. Joacob. A survey on authentification protocol. Available at the url http://www.cs.york.ac.uk/∼jac/papers/drareviewps.ps, 1997.

[CLC03] H. Comon-Lundh and V. Cortier. New decidability results for fragments of first-order logic and application to cryptographic protocols. In *14th Int. Conf. Rewriting Techniques and Applications (RTA'2003)*, volume 2706 of *LNCS*, 2003.

[CMR01] V. Cortier, J. Millen, and H. Rueß. Proving secrecy is easy enough. In *IEEE Computer Security Foundations Workshop*, pages 97–110, 2001.

[Coh00] Ernie Cohen. Taps: A first-order verifier for cryptographic protocols. In *Proceedings of the 13th IEEE Computer Security Foundations Workshop (CSFW'00)*, page 144. IEEE Computer Society, 2000.

[Com91] H. Comon. Disunification: A survey. In *Computational Logic: Essays in Honor of Alan Robinson*. MIT Press, Cambridge, MA, 1991.

[CS02] H. Comon and V. Shmatikov. Is it possible to decide whether a cryptographic protocol is secure or not? *Journal of Telecommunications and Information Technology*, 2002.

[DY83] D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[ES00] Neil Evans and Steve Schneider. Analysing time dependent security properties in CSP using PVS. In *ESORICS*, pages 222–237, 2000.

[FA01] M. Fiore and M. Abadi. Computing symbolic models for verifying cryptographic protocols. In *14th IEEE Computer Security Foundations Workshop (CSFW '01)*, pages 160–173, Washington - Brussels - Tokyo, June 2001. IEEE.

[Gon92] Li Gong. A security risk of depending on synchronized clocks. *Operating Systems Review*, 26(1):49–53, 1992.

[HNSY92] T.A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model-checking for real-time systems. In *Seventh Annual IEEE Symposium on Logic in Computer Science*, pages 394–406. IEEE Computer Society Press, 1992.

[JK91] J.-P. Jouannaud and C. Kirchner. Solving equations in abstract algebras: A rule-based survey of unification. In Jean-Louis Lassez and Gordon Plotkin, editors, *Computational Logic: Essays in Honor of Alan Robinson*. MIT-Press, 1991.

[Low97] Lowe. A hierarchy of authentication specifications. In *PCSFW: Proceedings of The 10th Computer Security Foundations Workshop*. IEEE Computer Society Press, 1997.

[MS01] J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *ACM Conference on Computer and Communications Security*, pages 166–175, 2001.

[Pau97] L. Paulson. Proving properties of security protocols by induction. In *IEEE Computer Security Foundations Workshop*, pages 70–83, 1997.

[RT01] M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *IEEE Computer Security Foundations Workshop*, 2001.

[THG98] J. Thayer, J. Herzog, and J. Guttman. Honest Ideals on Strand Spaces. In *IEEE Computer Security Foundations Workshop*, pages 66–78, 1998.

A Proofs

A.1 Definition of $\mathbf{lpt}(b, p)$

Definition A.1 *Let (b, p) be a term transducer. Then* the next term transducer in b from above that dominates p *(denoted by $lpt(b, p)$) is defined as follows:*

$$lpt(b,p) = \begin{cases} (b|_{1q}, 1q^{-1}p) & \text{if } \exists lpp(b|_1, 1^{-1}p) = q \\ undefined & otherwise \end{cases}$$

where $lpp(b, p)$ is defined in Section 5.3.

A.2 Proof of Proposition 4.1

Proposition 4.1. *Let E be a set of messages such that $E\langle w_i, S_i\rangle_I$ and let $(w_i, S_i)_{i\in I}$ be well-formed. Moreover, let m be a message with $E \vdash m$. Then, $m\langle w_i, S_i\rangle_I$.*

Proof Before tackling the proof, we introduce the following definition: We say that m is a *derivation-minimal counter-example*, if the following conditions are satisfied:

1. $E \vdash m$,
2. $\neg E\langle (w_i, S_i)_{i\in I}\rangle_K$ and
3. there is a derivation for $E \vdash m$ which does not contain any strict sub-derivation $E \vdash m'$ of a message m' with $\neg m'\langle (w_i, S_i)_{i\in I}\rangle_K$.

Assume that the assertion does not hold. Then, there exists a derivation-minimal counter-example m. The existence of m can be proved as follows. Take a derivation of $E \vdash m$ and let N_0 be its size. If m is not a derivation-minimal counter-example then there must exist a sub-derivation $E \vdash m'$ with $\neg m'\langle (w_i, S_i)_{i\in I}\rangle_K$. Clearly, the size N_1 of the derivation tree of m' is strictly smaller than N_0. Repeated application of the same argument must lead to a derivation-minimal counter-example as there are no strictly decreasing chains in $\mathbb{N}$.

Thus, let us come back to our derivation-minimal counter-example m. We derive a contradiction by case analysis on the last derivation step in $E \vdash m$.

1. $m \in E$. This, contradicts the assumption $E\langle (w_i, S_i)_{i\in I}\rangle_K$.
2. Case of encryption with a key from K. Thus, $m = \{m_1\}_{k_1}$, $E \vdash m_1$ and $E \vdash k_1$ with $k_1 \in K$. Since m is a derivation-minimal counter-example, we have $m_1\langle (w_i, S_i)_{i\in I}\rangle_K$ and $k_1\langle (w_i, S_i)_{i\in I}\rangle_K$. Since $\neg m\langle (w_i, S_i)_{i\in I}\rangle_K$, there exists $i \in I$ such that $\neg m\langle (w_i, S_i)\rangle_K$. It follows that $w_i \neq \epsilon$ and hence $w_i = (b, r).w$ and $m = b$ and $\neg b|_r\langle (w_i, S_i)\rangle_K$ $(*)$.

   If $\mathrm{lpt}(b, r)$ does not exist then we have $\neg m_1\langle (\epsilon, S_i)\rangle_K$, and hence, $\neg m_1\langle (w_i, S_i)\rangle_K$, which contradicts the derivation-minimality of m.

   So, let $(b_1, r_1) = \mathrm{lpt}(b, r)$. From definition, we have that $b|_r = b_1|_{r_1}$ $(**)$

   Since $(w_i, S_i)_{i\in I}$ is well-formed, there exists $j \in I$ such that either $b \in S_j$ or $w_j = (b_1, r_1).w$ and $S_i \subseteq S_j$.

   If we suppose that $b \in S_j$, since S_j is closed, we obtain that either $m_1 \in S_j$ or $k_1 \in S_j$ and hence either $\neg m_1\langle (w_j, S_j)\rangle_K$ or $\neg k_1\langle (w_j, S_j)\rangle_K$, contradiction.

   Hence $w_j = (b_1, r_1).w$ and $S_i \subseteq S_j$. From $m_1\langle (w_j, S_j)\rangle_K$, we obtain $b_1|_{r_1}\langle (w, S_j)\rangle_K$ $(***)$.

   From $(*)$, $(**)$ and $(***)$ we obtain a contradiction.
3. Case of encryption with a key which is not in K. Thus, $m = \{m_1\}_{k_1}$, $E \vdash m_1$ and $E \vdash k_1$ with $k_1 \notin K$. Since m is a derivation-minimal counter-example, we have $m_1\langle (w_i, S_i)_{i\in I}\rangle_K$, and then we obtain that $m\langle (w_i, S_i)_{i\in I}\rangle_K$, contradiction.
4. Case of pairing. Similar to the previous case.
5. Case of projection. This also contradicts the derivation-minimality assumption.

6. Case of decryption. Thus, $m_1 = \{m\}_{k_1}$, $E \vdash m_1$ and $E \vdash k_1^{-1}$. Since m is a derivation-minimal counter-example, we have $m_1\langle(w_i, S_i)_{i\in I}\rangle_K$ and $k_1^{-1}\langle(w_i, S_i)_{i\in I}\rangle_K$. If we suppose that $k_1 \notin K$, then we obtain that either $\neg m_1\langle(w_i, S_i)_{i\in I}\rangle_K$ or $m\langle(w_i, S_i)_{i\in I}\rangle_K$, contradiction. If $k_1 \in K$, since for all $i \in I$, S_i are closed, we obtain that $k_1^{-1} \in S_i$, contradiction with $k_1^{-1}\langle(w_i, S_i)_{i\in I}\rangle_K$.

□

A.3 Proof of proposition 4.2

In order to proof the Proposition 4.2 we start with proving the following proposition:

Proposition A.1 *Let m, s are two messages and E be a set of messages such that $\mathcal{K} \setminus K^{-1} \subseteq E$. If $\neg m\langle\epsilon\rangle s$ then $E, m \vdash s$.*

Proof By induction on the structure of m.

1. Case m atomic. Since $\neg m\langle\epsilon\rangle s$ we have $m = s$,so that $E, m \vdash s$.
2. Case of pair $m = (m_1, m_2)$. By definition, from $\neg m\langle\epsilon\rangle s$ we have either $m = s$ or $\neg m_1\langle\epsilon\rangle s \vee \neg m_2\langle\epsilon\rangle s$. If $m = s$ we have $m \vdash s$ else using the induction we have $E, m_1 \vdash s \vee E, m_2 \vdash s$ and we can conclude that $E, m \vdash s$.
3. Case of encrypted message with a key which is not in K, $m = \{m_1\}_{k_1}, k_1 \notin K$. By definition, we have either $m = s$ or $\neg m_1\langle\epsilon\rangle s$. if $m = s$ we have $E, m \vdash s$ else, using the induction we have $E, m_1 \vdash s$. From the hypothesis we know $\mathcal{K} \setminus K^{-1} \subseteq E$ and we are in the case where $k_1 \notin K$. Therefore, $k_1^{-1} \in E$ and consequently $E, \{m_1\}_{k_1} \vdash m_1$. Hence, we obtain $E, m \vdash s$.
4. Case of encrypted message with a key of K, $m = \{m_1\}_{k_1}, k_1 \in K$. By definition we have $\{m_1\}_{k_1}\langle\epsilon\rangle s$ is true for $k_1 \in K$ hence, we are not in the hypothesis of our proposition.

□

Corollary A.1 *Let s be a message and E be a set of messages such that $\mathcal{K} \setminus K^{-1} \subseteq E$. If $E \nvdash s$ then $E\langle\epsilon\rangle s$.*

Proof If we suppose that $\neg E\langle\epsilon\rangle s$ we have there is $m \in E$ such that $\neg m\langle\epsilon\rangle s$ and using Proposition A.1 we obtain that $E, m \vdash s$. But $m \in E$ hence we have $E \vdash s$, contradiction. □

Proposition 4.2. *Let m be a message and E a set of messages such that $\mathcal{K} \setminus K^{-1} \subseteq E$. Then, $E \nvdash m$ iff there exists a set of messages $A \in wc(m)$ s.t. $E\langle\epsilon\rangle A$.*

Proof "⇒": $E \nvdash m \Rightarrow \exists A \in \mathrm{wc}(m)$ s.t. $E\langle\epsilon\rangle A$

By induction on the structure of m.

1. Case m atomic. Then, $A = \mathrm{wc}(m) = \{\{m\}\}$ and using the Corollary A.1 we obtain that $E\langle\epsilon\rangle A$.
2. Case of pair $m = (m_1, m_2)$. From $E \nvdash m$ we have $E \nvdash m_1$ or $E \nvdash m_2$. Using the induction hypothesis we have $\exists A_1 \in \mathrm{wc}(m_1)$ such that $E\langle\epsilon\rangle A_1$ or $\exists A_2 \in \mathrm{wc}(m_2)$ such that $E\langle\epsilon\rangle A_2$. From $E \nvdash m$ and Corollary A.1 we obtain $E\langle\epsilon\rangle m$. Hence, for $A = \{m\} \cup A_1$ or $A = \{m\} \cup A_2$ we have $A \in \mathrm{wc}(m)$ and $E\langle\epsilon\rangle A$.
3. Case of encrypted message with a key K, $m = \{m_1\}_{k_1}$. Similar to the previous case.

"⇐" $\exists A \in \mathrm{wc}(m)$ s.t. $E\langle\epsilon\rangle A \Rightarrow E \nvdash m$

Let suppose that $E \vdash m$. From hypothesis we have $E\langle\epsilon\rangle A$ and from $A \in \mathrm{wc}(m)$ we have (ϵ, A) well-formed. Hence, using Proposition 4.1 we obtain that $m\langle\epsilon\rangle A$. But, from $A \in \mathrm{wc}(m)$ we have $m \in A$, contradiction. □

A.4 Definability of $t\langle w\rangle S$ in TSPL

We prove that any formulas of the form $t\langle w\rangle S$ is definable in TSPL.

Let s, t be terms, let w be a sequence of term transducers and let $\mathcal{J}(t, w, s)$ be defined as follows :

$$\mathcal{J}(t,w,s) = \begin{cases} x\langle w\rangle s & \text{if } t = x \in \mathcal{V} \\ \neg\mu(a,s) & \text{if } t = a \in \mathcal{A} \\ \mathcal{J}(t_1,w,s) \wedge \mathcal{J}(t_2,w,s) \wedge \neg\mu(t,s) & \text{if } t = (t_1,t_2) \\ \mathcal{J}(t_1,w,s) \wedge \neg\mu(t,s) & \text{if } t = \{t_1\}_k \wedge k \notin K \\ \neg\mu(t,s) & \text{if } t = \{t_1\}_k \wedge k \in K \wedge w = \epsilon \\ ((\mathcal{J}(b|_r,w_1,s) \wedge \mu(b,t)) \vee \neg\mu(b,t)) \wedge \neg\mu(t,s) & \text{if } t = \{t_1\}_k \wedge k \in K \wedge w = (b,r).w_1 \end{cases}$$

Then, $t\langle w\rangle s \equiv \mathcal{J}(t, w, s)$, i.e., both formulas are equivalent.

Proof First, notice that if $\mu(t_1, t_2) \neq \bot$, then $(\sigma, E, \nu, l) \in \mu(t_1, t_2)$ iff $t_1\sigma = t_2\sigma$, and if $\mu(t_1, t_2) = \bot$, then for any (σ, E, ν, l), it holds $t_1\sigma \neq t_2\sigma$. Now we prove by induction on $depth(t) + |w|$ that $t\langle w\rangle s \equiv \mathcal{J}(t, w, s)$.

1. If $t = x \in X$, then $\mathcal{J}(t, w, s) = x\langle w\rangle s = t\langle w\rangle s$.
2. If $t = a \in \mathcal{A}$, then $\mathcal{J}(t, w, s) = \neg\mu(a, s)$. Then we have $(\sigma, E, \nu, l) \in \neg\mu(a, s)$ iff $s\sigma \neq a$ iff $a\langle w\sigma\rangle s\sigma$ iff $(\sigma, E, \nu, l) \in a\langle w\rangle s$.
3. If $t = (t_1, t_2)$, then $\mathcal{J}(t, w, s) = \mathcal{J}(t_1, w, s) \wedge \mathcal{J}(t_2, w, s) \wedge \neg\mu(t, s)$. By induction hypothesis, we have $\mathcal{J}(t_1, w, s) \equiv t_1\langle w\rangle s$ and $\mathcal{J}(t_1, w, s) \equiv t_1\langle w\rangle s$. We obtain
   $(\sigma, E, \nu, l) \in \mathcal{J}(t, w, s)$ iff $(\sigma, E, \nu, l) \in t_1\langle w\rangle s \wedge t_2\langle w\rangle s \wedge \neg\mu(t, s)$ iff $t_1\sigma\langle w\sigma\rangle s\sigma \wedge t_2\sigma\langle w\sigma\rangle s\sigma \wedge t\sigma \neq s\sigma$ iff $t\sigma\langle w\sigma\rangle s\sigma$ iff $(\sigma, E, \nu, l) \in t\langle w\rangle s$.
4. The case $t = \{t_1\}_k \wedge k \notin K$ is similar to the previous one.
5. If $t = \{t_1\}_k \wedge k \in K \wedge w = \epsilon$, then we have $(\sigma, E, \nu, l) \in t\langle w\rangle s$ iff $t\sigma\langle\epsilon\rangle s\sigma$ iff $t\sigma \neq s\sigma$ iff $(\sigma, E, \nu, l) \in \neg\mu(t, s)$ iff $(\sigma, E, \nu, l) \in \mathcal{J}(t, w, s)$.
6. If $t = \{t_1\}_k \wedge k \in K \wedge w = (b, r).w_1$, then $\mathcal{J}(t, w, s) = \neg\mu(t, s) \wedge (\neg\mu(b, t) \vee (\mu(b, t) \wedge \mathcal{J}(b|_r, w_1, s)))$. By induction hypothesis, we have that $b|_r\langle w_1\rangle s \equiv \mathcal{J}(b|_r, w_1, s)$. We obtain
   $(\sigma, E, \nu, l) \in t\langle w\rangle s$ iff $t\sigma\langle\epsilon\rangle s\sigma \wedge (b\sigma = t\sigma \Rightarrow (b|_r)\sigma\langle w_1\sigma\rangle s\sigma)$ iff $t\sigma \neq s\sigma \wedge (b\sigma \neq t\sigma \vee (b\sigma = t\sigma \wedge (b|_r)\sigma\langle w_1\sigma\rangle s\sigma))$ iff $(\sigma, E, \nu, l) \in \neg\mu(t, s) \wedge (\neg\mu(b, t) \vee (\mu(b, t) \wedge b|_r\langle w_1\rangle s))$ iff $(\sigma, E, \nu, l) \in \neg\mu(t, s) \wedge (\neg\mu(b, t) \vee (\mu(b, t) \wedge \mathcal{J}(b|_r, w_1, s)))$ iff $(\sigma, E, \nu, l) \in \mathcal{J}(t, w, s)$.

□

A.5 Proof of Lemma 5.1

Lemma 5.1. *Let E be a set of terms, l be a label and let ρ and σ be ground substitutions such that $dom(\rho) = \tilde{x}$ and $(dom(\sigma) \cup var(E)) \cap \tilde{x} = \emptyset$. Then it holds $(\sigma, E, \nu, l) \in [\![F(t\rho)]\!]$ iff $E\sigma \vdash t(\sigma \oplus \rho)$.*

Proof

Since $(dom(\sigma) \cup var(E)) \cap \tilde{x} = \emptyset$ and using the Definition 4.4, we have

$(\sigma, E, \nu, l) \notin [\![F(t\rho)]\!]$ iff $(\sigma, E, \nu, l) \in \bigcup_{S' \in wc(t\rho)} [\![X\langle\epsilon\rangle S']\!]$ iff

$\exists S' \in wc(t\rho)$ *s.t.* $(\sigma, E, \nu, l) \in [\![X\langle\epsilon\rangle S']\!]$ iff

$\exists S' \in wc(t\rho)$ *s.t.* $E\sigma\langle\epsilon\rangle S'\sigma$ iff

$\exists S' \in wc((t\rho)\sigma)$ *s.t.* $E\sigma\langle\epsilon\rangle S'$ iff

$\exists S' \in wc(t(\rho \oplus \sigma))$ *s.t.* $E\sigma\langle\epsilon\rangle S'$ iff (using Proposition 4.2)

$E\sigma \nvdash t(\sigma \oplus \rho)$.

□

A.6 Proof of Lemma 5.2

Lemma 5.2. *Let t be a term, S a set of terms, w a sequence of term transducers, x a variable and $P_{x,t}$ the set of critical positions of x in t. Let*

$$\mathcal{K}(t,x,w,S) = X\langle w\rangle S \wedge \bigwedge_{p=lpp(t,p_x),p_x\in P_{x,t}} \mathcal{H}(X\langle(t|_p,p^{-1}p_x).w\rangle S).$$

Let E be a set of terms, l and l' labels, and ρ, σ ground substitutions such that $dom(\rho)=\tilde{x}$, $x\in\tilde{x}$, $(dom(\sigma)\cup var(E))\cap\tilde{x}=\emptyset$. Let Φ a well-formed formula such that whenever $E\sigma\vdash\ t(\sigma\oplus\rho)$, it holds

$$(\sigma\oplus\rho,E,l')\in[\![(X,x)\langle w\rangle S]\!] \text{ iff } (\sigma,E,l)\in[\![\Phi]\!]$$

Then $[\![\Phi]\!]=[\![\rho(\mathcal{K}(t,x,w,S))]\!]$.

Proof "$\Leftarrow$"

Let suppose that $(\sigma,E,\nu,l)\in[\![\rho(\mathcal{K}(t,x,w,S))]\!]$. Since $(\sigma,E,\nu,l)\in[\![X\langle w\rho\rangle S\rho]\!]$, it follows that $E\sigma\langle w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$.

It remains to prove that $\rho(x)\langle w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$.

We have that $E\sigma\vdash\ t(\sigma\oplus\rho)$.

From $(\sigma,E,\nu,l)\in[\![\mathcal{H}(X\langle(t|_p,p^{-1}p_x).w\rangle S)]\!]$ it follows that $E\sigma\langle(t(\sigma\oplus\rho)|_p,p^{-1}p_x).w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$. By construction, the formula $\mathcal{H}(X\langle(t|_p,p^{-1}p_x).w\rangle S)$ is well-formed. Using Corollary 4.1, we obtain $t(\sigma\oplus\rho)\langle(t(\sigma\oplus\rho)|_p,p^{-1}p_x).w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$, and from Definition 4.1 we obtain $\rho(x)\langle w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$.

"$\Rightarrow$"

We have that $(\sigma,E,\nu,l')\in[\![\rho(x)\langle w\rho\rangle S\rho\wedge X\langle w\rho\rangle S\rho]\!]$. Let suppose that $\forall p_x\in P_{x,t}\exists\text{lpt}(t,p_x)$.

We have to prove that $(\sigma,E,\nu,l)\in[\![X\langle w\rho\rangle S\rho]\!]$ and $(\sigma,E,\nu,l)\in[\![\mathcal{H}(X\langle(t|_p,p^{-1}p_x).w\rangle S)]\!]$.

From $(\sigma,E,\nu,l')\in[\![\rho(x)\langle w\rho\rangle S\rho\wedge X\langle w\rho\rangle S\rho]\!]$ we obtain that $E\sigma\langle w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$ and $\rho(x)\langle w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$.

It remains to prove that $(\sigma,E,\nu,l)\in[\![\mathcal{H}((X\langle(t|_p,p^{-1}p_x).w\rangle S)]\!]$. Firstly we prove that $E\sigma\langle(t(\sigma\oplus\rho)|_p,p^{-1}p_x).w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$.

If we suppose that $\neg E\sigma\langle(t(\sigma\oplus\rho)|_p,p^{-1}p_x).w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$ it means that $\exists m\in E$ such that $\neg m\sigma\langle(t(\sigma\oplus\rho)|_p,p^{-1}p_x).w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$, and using the Definition 4.1 we obtain that either $\neg m\sigma\langle w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$ or $\neg\rho(x)\langle w(\sigma\oplus\rho)\rangle S(\sigma\oplus\rho)$, contradiction.

Now the assertion follows from the Proposition 4.3.

The case $\exists p_x\in P_{x,t}\ \nexists\text{lpt}(t,p_x)$ is similar.

□

A.7 Proof of Proposition 5.2

To prove the Proposition 5.2, we need an auxiliary Lemma.

Lemma A.1 *Let $\rho\in\Gamma(\tilde{x})$, and let φ an atomic term formula. Then $\rho(\mathbf{Pre}(l\ \stackrel{g,\mathcal{R},?t(\tilde{x})}{\longrightarrow}\ l',\varphi))\equiv\rho(g)\wedge(pc=l)\wedge F(t\rho)\wedge\rho(\varphi)$*

Proof By an analysis by cases on φ. The only non-trivial case is when $\varphi=(X,x)\langle w\rangle S$ and $x\in\tilde{x}$, and the assertion follows as a direct consequence of Lemma 5.1 and Lemma 5.2. □

Proposition 5.3. *For any input action α and atomic term formula φ,*

$$pre(\alpha,[\![\varphi]\!])=[\![\mathbf{Pre}(\alpha,\varphi)]\!].$$

Proof In the sequel l'' is a label, E is a set of terms and σ is a ground substitution such that $\tilde{x} \cap (dom(\sigma) \cup var(E)) = \emptyset$.

$(\sigma, E, \nu, l'') \in pre(l \overset{g,\mathcal{R},?t(\tilde{x})}{\longrightarrow} l', [\![\varphi]\!])$ iff

$\exists \rho \in \Gamma(\tilde{x})$ s.t. $l'' = l \wedge E\sigma \vdash t(\sigma \oplus \rho) \wedge [\![g]\!]_{\nu,\sigma\oplus\rho} = 1 \wedge (\sigma \oplus \rho, E, \nu l'') \in [\![\varphi]\!]$ iff

$\exists \rho \in \Gamma(\tilde{x})$ s.t.$(\sigma, E, \nu, l'') \in [\![pc = l \wedge \rho(g)]\!] \wedge (\sigma, E, \nu, l'') \in [\![F(t\rho)]\!] \wedge (\sigma, E, \nu l'') \in [\![\rho(\varphi)]\!]$ iff

$\exists \rho \in \Gamma(\tilde{x})$ s.t.$(\sigma, E, \nu, l'') \in [\![\rho(g) \wedge (pc = l) \wedge F(t\rho) \wedge \rho(\varphi)]\!]$ iff

$\exists \rho \in \Gamma(\tilde{x})$ s.t.$(\sigma, E, \nu, l'') \in [\![\rho(\mathbf{Pre}(l \overset{g,\mathcal{R},?t(\tilde{x})}{\longrightarrow} l', \varphi))]\!]$ iff

$(\sigma, E, \nu, l'') \in [\![\mathbf{Pre}(l \overset{g,\mathcal{R},?t(\tilde{x})}{\longrightarrow} l', \varphi)]\!]$

□

A.8 Computation of predecessors for a sequence of actions

In this subsection, we give an example that shows how we compute the set of predecessors with respect to a simple protocol.

Example A.1 *Let* $\alpha_0 = l_0 \overset{\top,\emptyset,!\{c\}_k}{\longrightarrow} l_1$, $\alpha_1 = l_1 \overset{\top,\{d\},!\{c\}_k}{\longrightarrow} l_2$,$\alpha_2 = l_2 \overset{g_2,\emptyset,?\{T\}_k}{\longrightarrow} l_3$, $\alpha_3 = l_3 \overset{\top,\emptyset,!s}{\longrightarrow} l_4$ *where c and d are clocks, k is a symmetric key (intended to remain secret for the intruder), s is a message (the secret) and* $g_2 \equiv d = 1 \wedge -c + T < -1$. *Let* $\Phi \overset{def}{=} X\langle \not\in \rangle s$ *be the formula that represents the "bad configurations" (where secret s is known to the intruder). Now let* $\Pi_1 = \alpha_1\alpha_2\alpha_3$ *and* $\Pi_0 = \alpha_0\alpha_1\alpha_2\alpha_3$ *are two protocols. We show that* Π_1 *is secure w.r.t. to formula* Φ*, while the same assertion does not hold for* Π_2. *For sake of simplicity, we work modulo* $\equiv$.

Then

$\mathbf{Pre}(\overset{\tau}{\longrightarrow}, X\langle \not\in \rangle s) = X\langle \not\in \rangle s$.

$\mathbf{Pre}(\alpha_3, X\langle \not\in \rangle s) = \top \wedge pc = l_3 \wedge (X, s)\langle \not\in \rangle s \equiv pc = l_3$

$\mathbf{Pre}(\overset{\tau}{\longrightarrow}, pc = l_3) = pc = l_3$

$\mathbf{Pre}(\alpha_2, pc = l_3) = \Phi_1$ *where*

$$\Phi_1 \equiv d = 1 \wedge -c + T < -1 \wedge pc = l_2 \wedge X\langle \not\in \rangle \{\{T\}_k, T\} \wedge X\langle \not\in \rangle \{\{T\}_k, k\}$$

$\mathbf{Pre}(\overset{\tau}{\longrightarrow}, \Phi_1) = \Phi_2$ *where*

$$\Phi_2 \equiv (d \leq 1) \wedge d - c + T < 0 \wedge pc = l_2 \wedge X\langle \not\in \rangle \{\{T\}_k, T\} \wedge X\langle \not\in \rangle \{\{T\}_k, k\}$$

$\mathbf{Pre}(\alpha_1, \Phi_2) = \Phi_3$ *where* $\Phi_3 \equiv$

$$(0 \leq 1) \wedge 0 - c + T < 0 \wedge pc = l_1 \wedge (X, \{T_c\}_k)\langle \not\in \rangle \{\{T\}_k, T\} \wedge (X, \{T_c\}_k)\langle \not\in \rangle \{\{T\}_k, k\} \wedge T_c = c$$

$$\equiv -c + T < 0 \wedge pc = l_1 \wedge T_c = c \wedge T < T_c \wedge ((X\langle \not\in \rangle \{\{T\}_k, T\} \wedge X\langle \not\in \rangle \{\{T\}_k, k\}) \vee T_c = T)$$

$$\equiv -c + T < 0 \wedge pc = l_1 \wedge T_c = c \wedge T < T_c \wedge (X\langle \not\in \rangle \{\{T\}_k, T\} \wedge X\langle \not\in \rangle \{\{T\}_k, k\})$$

$\mathbf{Pre}(\overset{\tau}{\longrightarrow}, \Phi_3) = \Phi_4$ *where*

$$\Phi_4 \equiv pc = l_1 \wedge c \leq T_c \wedge T < T_c \wedge X\langle \not\in \rangle \{\{T\}_k, T\} \wedge X\langle \not\in \rangle \{\{T\}_k, k\}$$

$\mathbf{Pre}(\alpha_0, \Phi_4) = \Phi_5$ *where*

$$\Phi_5 \equiv pc = l_0 \wedge c \leq T_c \wedge T < T_c \wedge (X, \{T'_c\}_k)\langle \not\in \rangle \{\{T\}_k, T\} \wedge (X, \{T'_c\}_k)\langle \not\in \rangle \{\{T\}_k, k\} \wedge T'_c = c$$

$$\equiv pc = l_0 \wedge c \leq T_c \wedge T < T_c \wedge T'_c = c \wedge T'_c < T_c \wedge ((X\langle \not\in \rangle \{\{T\}_k, T\} \wedge X\langle \not\in \rangle \{\{T\}_k, k\}) \vee T'_c = T)$$

$\mathbf{Pre}(\overset{\tau}{\longrightarrow}, \Phi_5) = \Phi_6$ *where*

$$\Phi_6 \equiv pc = l_0 \wedge c \leq T_c \wedge c \leq T'_c \wedge T < T_c \wedge T'_c < T_c \wedge ((X\langle \not\in \rangle \{\{T\}_k, T\} \wedge X\langle \not\in \rangle \{\{T\}_k, k\}) \vee T'_c = T)$$

Hence, we obtain

$$pre(\Pi_1, X\langle\not\in\rangle s) \equiv pc = l_1 \wedge c \leq T_c \wedge T < T_c \wedge X\langle\not\in\rangle\{\{T\}_k, T\} \wedge X\langle\not\in\rangle\{\{T\}_k, k\}$$

and

$$pre(\Pi_0, X\langle\not\in\rangle s) \equiv pc = l_0 \wedge c \leq T_c \wedge c \leq T'_c \wedge T < T_c \wedge T'_c < T_c \wedge ((X\langle\not\in\rangle\{\{T\}_k, T\} \wedge X\langle\not\in\rangle\{\{T\}_k, k\}) \vee T'_c = T)$$

Since we supposed that k is a secret symmetric key (i.e.$X\langle\not\in\rangle k$), if there is no any message of the form $\{T''\}_k$ known initially to the intruder, the protocol Π_1 is secure with respect to the secrecy of s. On the contrary, protocol Π_0 is unsecure. If we pick T_c, and T'_c such that $T < T_c \wedge T'_c < T_c \wedge T'_c = T$, then we obtain an attack, that corresponds to the fact that the first message sent by our participant can be replayed successfully by the intruder (it satisfies the time constraints), while the same is not true for the second sent message.

A.9 Decidability of the existential fragment of TSPL

Theorem A.1 *Application of the rules of Table 7 terminates in a solved form.*

Proof let us first briefly mention how each rule contributes in reaching a normal form:

1. Rule **Eliminate** X can be applied only once.
2. Rule **D1** decreases the number of sub-formulae of the form $t\langle w\rangle s$ but may introduce equalities and disequalities as well as new formulae of the form $x\langle w\rangle s$.
3. Rule **D2** decreases the length of w in sub-formulae of the form $x\langle w\rangle s$ but introduces new formulae of the form $t\langle w\rangle s$.
4. Rule **D3** decreases the number of equalities (disequalities) where the two members are not variables.
5. Rules **Occur-check** and **Replacement** eliminate a variable.

Now, to prove termination we need to introduce interpretation functions which are intended to decrease by applications of the rules:

- $f_1(\varphi)$ is the number of occurrences of X (in φ).
- $f_2(\varphi)$ is the cardinality of $var(\varphi)$.
- $f_3(\varphi)$ is the multi-set of pairs $(|w|, |t|)$, where $t\langle w\rangle s$ is a sub-formula. For the variation of this function, we take the multi-set extension of the lexicographic ordering on $\mathbb{N}^2$. This is a well-ordering.
- $f_4(\varphi)$ is the number of equations (disequations) where both members are not variables.
- $f_5(\varphi)$ is the size of φ.

Figure 1 summarizes the variation of each function by the transformation rules: Thus, if we define

	f_1	f_2	f_3	f_4	f_5
T	$=$	$\leq$	$=$	$=$	$<$
D_3	$=$	$=$	$=$	$<$	
$D_1 + D_2$	$=$	$=$	$<$		
R	$=$	$<$			
OC	$=$	$<$			
EX	$<$				

Figure 1: Variation of the ranking functions

$F(\varphi) = (f_1(\varphi), \cdots, f_5(\varphi))$ then $F(\varphi)$ decreases with respect to lexicographic ordering by each rule. Hence, termination of the rules.
It remains now to show that if no rule can be applied then the obtained formula is in solved form. This proof is easy and tedious and is not given in this abstract. □