NEW FUNCTIONS FOR SECRECY ON REAL PROTOCOLS

Jaouhar Fattahi[1] and Mohamed Mejri[1] and Hanane Houmani[2]

[1]LSI Group, Laval University, Quebec, Canada
[2]University Hassan II, Morocco

ABSTRACT

In this paper, we present new functions for secrecy in cryptographic protocols:the witness-functions. A witness-function is a protocol-dependent function that is able to prove the correctness of a protocol through its growth. It bases its calculation on the static part of a message only in a role-based specification by using derivation techniques. We show here how to build them. Then, we run an analysis on two real protocols. First, we run an analysis on NSL protocol and we prove that it is correct with respect to the property of secrecy. Then, we run an analysis on a variation of Needham-Schroeder protocol in which we show that a witness-function could even help to discover flaws.

KEYWORDS

Cryptographic Protocols, Role-based specification, Secrecy

1. INTRODUCTION

In this paper, we present a new class of functions to analyze cryptographic protocols statically for the property of secrecy: the witness-functions. Intuitively, an increasing protocol keeps the secret. That means that if the security of all atomic messages exchanged in the protocol does not decay between receiving and sending steps in the protocol, the secret is preserved. For that, we need reliable metrics to estimate the security of atomic messages. This approach has been adopted in some prior works. In [1], Steve Schneider presented the notion of rank-functions as tools to analyze protocols in CSP [2, 3]. They were efficient in analyzing many protocols such Needham-Schroeder protocol. Nevertheless, a such analysis dictates the protocol implementation in CSP algebra. In addition, building rank-functions is not an easy task and their existence is not certain [4]. In [5] Abadi, by utilizing Spi-Calculus [6, 7], asserted that: "If a protocol typechecks, then it keeps the secret". For that, he restricted the exchanged messages to have strictly the following types: {secret, public, any, confounder} in order to easily know the security level of every component in. This approach cannot analyze prior protocols that had been designed with no respect to this condition.

Similarly, Houmani et al. [8–11] presented universal functions that they named the interpretation functions to statically analyze a protocol. An interpretation function needs to meet some conditions to be "enough good" for the analysis. Naturally, less we have restrictions on functions,

Natarajan Meghanathan et al. (Eds) : ICCSEA, SPPR, VLSI, WiMoA, SCAI, CNSA, WeST - 2014
pp. 229–250, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4728

more we have the chance to define functions and therefore to have the chance to prove the correctness of protocols. In fact, one function may not succeed to prove the growth of a protocol but another function may. In this respect, we note that the conditions on functions were very restrictive. That's why only two functions had been given: DEK and DEKAN.

We think that the condition of full-invariance by substitution, which enables an analysis run on messages of the generalized roles (messages with variables) to be propagated to valid traces (closed messages), is the most limitative one. From the moment that the goal of our approach is to build as more functions as we can, we believe that if we liberate a function from this condition, we will be able to build more functions. However, liberating a function from a condition may oblige us to take extra precautions when using it.

In this paper, we present the witness-functions as new metrics to analyze cryptographic protocols. We give the way to build them. We show that a witness-function provides two bounds that allow us to pass beyond the limitative condition of full-invariance by substitution by introducing the notion of derivative messages. We exhibit the theorem of analysis with the witness-functions that gives a criterion for the protocol correctness. Finally, we run an analysis on two real protocols. First, we run an analysis on NSL protocol where we prove that it is correct with respect to the property of secrecy. Then, we run an analysis on a variation of Needham-Schroeder protocol in which we show that a witness-function could even help to locate flaws.

2. PRELIMINARY AND NOTATIONS

Here, we give some conventions and notations that we use in this paper.

+ We denote by $\mathcal{C} = \langle \mathcal{M}, \xi, \models, \mathcal{K}, \mathcal{L}^{\sqsupset}, \ulcorner . \urcorner \rangle$ the context of verification in which our analysis is run. It contains the parameters that affect the analysis of a protocol:
  - $\mathcal{M}$: is a set of messages built from the signature $\langle \mathcal{N}, \Sigma \rangle$ where $\mathcal{N}$ is a set of atomic names (nonces, keys, principals, etc.) and Σ is a set of functions (enc: encryption, dec: decryption, $pair$: concatenation (that we denote by "." here), etc.). i.e. $\mathcal{M} = T_{\langle \mathcal{N}, \Sigma \rangle}(\mathcal{X})$. We denote by Γ the set of substitutions from $\mathcal{X} \rightarrow \mathcal{M}$. We denote by $\mathcal{A}$ all the atomic messages in $\mathcal{M}$, by $\mathcal{A}(m)$ the set of atomic messages (or atoms) in m and by $\mathcal{I}$ the set of principals including the intruder I. We denote by k^{-1} the reverse form of a key k and we assume that $(k^{-1})^{-1} = k$.
  - ξ : is the equational theory in which the algebraic properties of the functions in Σ are described by equations. e.g. $dec(enc(x, y), y^{-1}) = x$.
  - $\models_{\mathcal{C}}$: is the inference system of the intruder under the equational theory. Let M be a set of messages and m a message. $M \models_{\mathcal{C}} m$ means that the intruder is able to infer m from M using her capacity. We extend this notation to traces as follows: $\rho \models_{\mathcal{C}} m$ means that the intruder can infer m from the messages exchanged in the trace ρ. We suppose that the intruder has the full control of the net as described by Dolev-Yao model in [12]. That is to say that she can intercept, delete, redirect and modify messages. She knows the public keys of all agents. She knows her private keys and the keys that she shares with other agents. She can encrypt or decrypt any message with known keys. Generically, the intruder has the following rules of building messages:

$$(int) : \frac{\square}{M \models_{\mathcal{C}} m} [m \in M \cup K(I)]$$

$$(op) : \frac{M \models_{\mathcal{C}} m_1, \ldots, M \models_{\mathcal{C}} m_n}{M \models_{\mathcal{C}} f(m_1, \ldots, m_n)} [f \in \Sigma]$$

$$(eq) : \frac{M \models_{\mathcal{C}} m', m' =_{\mathcal{C}} m}{M \models_{\mathcal{C}} m}, \text{with } (m' =_{\mathcal{C}} m) \equiv (m' =_{\xi_{(\mathcal{C})}} m)$$

Example 2.1

The intruder capacity can be described by the following rules:

$$(int) : \frac{\square}{M \models_{\mathcal{C}} m}[m \in M \cup K(I)]$$

$$(concat) : \frac{M \models_{\mathcal{C}} m_1, M \models_{\mathcal{C}} m_2}{M \models_{\mathcal{C}} m_1.m_2}$$

$$(deconcat) : \frac{M \models_{\mathcal{C}} m_1.m_2}{M \models_{\mathcal{C}} m_i}[i \in \{1,2\}]$$

$$(dec) : \frac{M \models_{\mathcal{C}} k, M \models_{\mathcal{C}} m_k}{M \models_{\mathcal{C}} m}$$

$$(enc) : \frac{M \models_{\mathcal{C}} k, M \models_{\mathcal{C}} m}{M \models_{\mathcal{C}} \{m\}_k}$$

In this example, from a set of messages, an intruder can infer any message in this set. She can encrypt any message when she holds the encryption key. She can decrypt any message when she holds the decryption key and concatenate any two messages and deconcatenate them.

- $\mathcal{K}$: is a function from $\mathcal{I}$ to $\mathcal{M}$, that returns to any agent a set of atomic messages describing her initial knowledge. We denote by $K_{\mathcal{C}}(I)$ the initial knowledge of the intruder, or simply $K(I)$ where the context is obvious.
- $\mathcal{L}^{\sqsupseteq}$: is the lattice of security $(\mathcal{L}, \sqsupseteq, \sqcup, \sqcap, \bot, \top)$ used to assign security levels to messages. An example of a lattice is $(2^{\mathcal{I}}, \subseteq, \cap, \cup, \mathcal{I}, \emptyset)$ that will be used to attribute to an atomic message α the set of agents that are authorized to know it.
- $\ulcorner . \urcorner$: is a partial function that attributes a value of security (or type) to a message in $\mathcal{M}$. Let M be a set of messages and m a message. We write $\ulcorner M \urcorner \sqsupseteq \ulcorner m \urcorner$ if $\exists m' \in M . \ulcorner m' \urcorner \sqsupseteq \ulcorner m \urcorner$

Our analysis is performed in a role-based specification. A role-based specification is a set of generalized roles. A generalized role is an abstraction of the protocol where the emphasis is put on a specific agent and where all the unknown messages, and on which the agent cannot carry out any verification, are substituted by variables. An exponent i (the session identifier) is added to a fresh message to say that these components change values from one run to another. A generalized role interprets how a particular agent perceives the exchanged messages. It is extracted from a protocol as follows:

– Extract the roles from the protocol.
– Substitute the unknown messages by fresh variables for each role.

The roles are extracted as follows:

- For each agent, extract from the protocol all the steps in which this principal is participating. Then, add to this abstraction a session identifier i in the steps identifiers and in the fresh values. For example, from the variation of Woo and Lam protocol given in the Table 1, we extract three roles, denoted by R_A (for the agent A), R_B (for the agent B), and R_S (for the agent S).
- Introduce an intruder I to express the fact that the received messages and the sent messages are probably sent or received by the intruder.

- Finally, extract all prefixes from those roles where a prefix ends by a sending step.

$$
\begin{array}{ll}
p = & \langle 1, A \to B : A \rangle. \\
& \langle 2, B \to A : N_b \rangle. \\
& \langle 3, A \to B : \{N_b, k_{ab}\}_{k_{as}} \rangle. \\
& \langle 4, B \to S : \{A, \{N_b, k_{ab}\}_{k_{as}}\}_{k_{bs}} \rangle. \\
& \langle 5, S \to B : \{N_b, k_{ab}\}_{K_{bs}} \rangle
\end{array}
$$

Table 1: The Woo and Lam Protocol

From the roles, we generate the generalized roles. In a generalized role, unknown messages are substituted by variables to express that the agent cannot be sure about its integrity or its origin. In the Woo and Lam protocol, the generalized role of S is:

$$
\begin{array}{lllllll}
\mathcal{S}^1_G = & \langle i.4, & I(B) & \to & S & : & \{A, \{U, V\}_{k_{as}}\}_{k_{bs}} \rangle. \\
& \langle i.5, & S & \to & I(B) & : & \{U, V\}_{k_{bs}} \rangle
\end{array}
$$

The generalized roles of A are:

$$
\mathcal{A}^1_G = \langle i.1, \quad A \to I(B) : A \rangle
$$

$$
\begin{array}{lllllll}
\mathcal{A}^2_G = & \langle i.1, & A & \to & I(B) & : & A \rangle. \\
& \langle i.2, & I(B) & \to & A & : & X \rangle. \\
& \langle i.3, & A & \to & I(B) & : & \{X, k^i_{ab}\}_{k_{as}} \rangle
\end{array}
$$

The generalized roles of B are:

$$
\begin{array}{lllllll}
\mathcal{B}^1_G = & \langle i.1, & I(A) & \to & B & : & A \rangle. \\
& \langle i.2, & B & \to & I(A) & : & N_b \rangle \\
\mathcal{B}^2_G = & \langle i.1, & I(A) & \to & B & : & A \rangle. \\
& \langle i.2, & B & \to & I(A) & : & N_b \rangle. \\
& \langle i.3, & I(A) & \to & B & : & Y \rangle. \\
& \langle i.4, & B & \to & I(S) & : & \{A, Y\}_{k_{bs}} \rangle \\
\mathcal{B}^3_G = & \langle i.1, & I(A) & \to & B & : & A \rangle. \\
& \langle i.2, & B & \to & I(A) & : & N_b \rangle. \\
& \langle i.3, & I(A) & \to & B & : & Y \rangle. \\
& \langle i.4, & B & \to & I(S) & : & \{A, Y\}_{k_{bs}} \rangle. \\
& \langle i.5, & I(S) & \to & B & : & \{N^i_b, Z\}_{k_{bs}} \rangle
\end{array}
$$

Thus, the role-based specification of the protocol in the Table 1 is $\mathcal{R}_G(p) = \{\mathcal{A}^1_G, \mathcal{A}^2_G, \mathcal{B}^1_G, \mathcal{B}^2_G, \mathcal{B}^3_G, \mathcal{S}^1_G\}$. The role-based specification is used to express the notion of valid traces of a protocol. More details about the role-based specification could be found in [13–16].

+ A valid trace is an interleaving of substituted generalized roles where each message sent by the intruder can be generated by her using her capacity and by the received messages. We denote by $[\![p]\!]$ the set of valid traces generated by p.
+ We denote by $\mathcal{M}_p^{\mathcal{G}}$ the set of messages (with variables) in $R_G(p)$, by $\mathcal{M}_p$ the set of closed messages generated by substitution in $\mathcal{M}_p^{\mathcal{G}}$. We denote by R^+ (respectively R^-) the set of sent messages (respectively received messages) by a honest agent in the role R. Conventionally, we devote the uppercase symbols for sets or sequences of elements and the lowercase for single elements. For example, M denotes a set of messages, m a single message, R a role composed of a sequence of steps, r a step and $R.r$ the role ending by the step r.
+ In our analysis, no restriction on the size of messages or the number of sessions in the protocols is made.

3. INCREASING PROTOCOLS DO NOT REVEAL SECRETS

To analyze a protocol, we need interpretation functions to estimate the security level of every atomic message. In this section, we give sufficient conditions on a function F to guarantee that it is enough good (or reliable) to run an analysis and we show that an increasing protocol is correct with respect to the secrecy property when analyzed with such functions.

3.1 C-reliable interpretation functions

An interpretation function F is said well-formed when it returns the bottom value in the lattice, denoted by $\bot$, for an atomic message α that appears in clear. It returns for it in the union of two sets, the minimum "$\sqcap$" of the two values calculated in each set separately. It returns the top value, denoted by "$\top$", if it does not appear in this set. These facts are expressed by the definition 3.1.

Definition 3.1. (Well-formed interpretation function)
Let F be an interpretation function and $\mathcal{C}$ a context of verification.
F is well-formed in $\mathcal{C}$ if:
$\forall M, M_1, M_2 \subseteq \mathcal{M}, \forall \alpha \in \mathcal{A}(\mathcal{M})$:

$$\begin{cases} F(\alpha, \{\alpha\}) & = & \bot \\ F(\alpha, M_1 \cup M_2) & = & F(\alpha, M_1) \sqcap F(\alpha, M_2) \\ F(\alpha, M) & = & \top, \text{ if } \alpha \notin \mathcal{A}(M) \end{cases}$$

An interpretation function F is said full-invariant-by-intruder if when it attributes a security level to a message α in a set of messages M, the intruder can never produce another message m that decrease this level (i.e. $F(\alpha, m) \sqsupseteq F(\alpha, M)$) using her capacity in the context of verification, except when α is intended to be known by the intruder (i.e. $\ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner$). This fact is expressed by the definition 3.2.

Definition 3.2. (Full-invariant-by-intruder interpretation function)
Let F be an interpretation function and $\mathcal{C}$ a context of verification.
F is full-invariant-by-intruder in $\mathcal{C}$ if:
$\forall M \subseteq \mathcal{M}, m \in \mathcal{M}. M \models_{\mathcal{C}} m \Rightarrow \forall \alpha \in \mathcal{A}(m). (F(\alpha, m) \sqsupseteq F(\alpha, M)) \vee (\ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner)$

An interpretation function F is said reliable if it is well-formed and full-invariant-by-intruder. This fact is expressed by the definition 3.3.

Definition 3.3. (Reliable interpretation function)
Let F be an interpretation function and C a context of verification.
F is C-reliable if F is well-formed and F is full-invariant-by-intruder in C.

A protocol p is said F-increasing when every principal generates continuously valid traces (substituted generalized roles) that never decrease the security levels of received components. The estimation of the value of security of every atom is performed by F. This fact is expressed by the definition 3.4.

Definition 3.4. (F-increasing protocol)
Let F be an interpretation function, $\mathcal{C}$ a context of verification and p a protocol.
p is F-increasing in $\mathcal{C}$ if:
$\forall R.r \in R_G(p), \forall \sigma \in \Gamma : \mathcal{X} \rightarrow \mathcal{M}_p$ we have:

$$\forall \alpha \in \mathcal{A}(\mathcal{M}_p).F(\alpha, r^{+}\sigma) \sqsupseteq \ulcorner \alpha \urcorner \sqcap F(\alpha, R^{-}\sigma)$$

A secret disclosure consists in manipulating a valid trace of the protocol (denoted by $[\![p]\!]$) by the intruder using her knowledge $K(I)$ in a context of verification $\mathcal{C}$, to deduce a secret α that she is not intended to know (expressed by: $\ulcorner K(I) \urcorner \not\sqsupseteq \ulcorner \alpha \urcorner$). This fact is expressed by the definition 3.5.

Definition 3.5. (Secret disclosure)
Let p be a protocol and $\mathcal{C}$ a context of verification.
We say that p discloses a secret $\alpha \in \mathcal{A}(\mathcal{M})$ in $\mathcal{C}$ if:

$$\exists \rho \in [\![p]\!].(\rho \models_{\mathcal{C}} \alpha) \wedge (\ulcorner K(I) \urcorner \not\sqsupseteq \ulcorner \alpha \urcorner)$$

Lemma 3.6.
Let F be a $\mathcal{C}$-reliable interpretation function and p an F-increasing protocol.
We have:

$$\forall m \in \mathcal{M}.[\![p]\!] \models_{\mathcal{C}} m \Rightarrow \forall \alpha \in \mathcal{A}(m).(F(\alpha, m) \sqsupseteq \ulcorner \alpha \urcorner) \vee (\ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner)$$

See the proof 4 in [17]

The lemma 3.6 says that for any atom in a message produced by an increasing protocol, its security level returned by a reliable interpretation function is kepts greater or equal than its initial value in the context, if the intruder is not initially allowed to know it. Hence, initially the atom has a certain level of security. This value cannot be decreased by the intruder using her knowledge and the received messages since it is full-invariant-by-intruder. In every new step of a valid trace, involved messages are better protected since the protocol is increasing. The proof is then run by induction on the size of the trace using the reliability properties of the interpretation function in every step of the induction.

Theorem 3.7. (Theorem of Correctness of Increasing Protocols)
Let F be a C-reliable interpretation function and p a F-increasing protocol.
p is C-correct with respect to the secrecy property

Proof.

Let's suppose that p discloses an atomic secret α.

From the definition 3.5 we have:

$$\exists \rho \in [\![p]\!].(\rho \models_{\mathcal{C}} \alpha) \wedge (\ulcorner K(I) \urcorner \not\sqsupseteq \ulcorner \alpha \urcorner) \quad (1)$$

Since F is a $\mathcal{C}$-reliable interpretation function and p an F-increasing protocol, we have from the lemma 3.6:

$$(F(\alpha, \alpha) \sqsupseteq \ulcorner \alpha \urcorner) \vee (\ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner) \quad (2)$$

From 1 and 2, we have:

$$F(\alpha, \alpha) \sqsupseteq \ulcorner \alpha \urcorner \quad (3)$$

Since F is well-formed in $\mathcal{C}$, then:

$$F(\alpha, \alpha) = \bot \quad (4)$$

From 3 and 4 we have:

$$\bot = \ulcorner \alpha \urcorner \quad (5)$$

5 is impossible because it is contradictory with: $\ulcorner K(I) \urcorner \not\sqsupseteq \ulcorner \alpha \urcorner$ in 1.

Then p is C-correct with respect to the secrecy property

The theorem 3.1 asserts that an increasing protocol is correct with respect to the secrecy property when analyzed with a reliable interpretation function. It is worth saying that compared to the sufficient conditions stated in [11], we have one less. Thus, in [11], Houmani demanded from the interpretation function an additional condition: the full-invariance by substitution. That's to say, interpretation function has also to resist to the problem of substitution of variables. Here, we liberate our functions from this limitative condition in order to be able to build more of them. We rehouse this condition in our new definition of an increasing protocol which is required now to be increasing on valid traces (closed messages) rather than messages of the generalized roles (message with variables). Therefore, the problem of substitutions is transferred to the protocol and becomes less difficult to handle.

4. CONSTRUCTION OF RELIABLE INTERPRETATION FUNCTIONS

As seen in the previous section, to analyze a protocol we need reliable interpretation functions to estimate the level of security of any atom in a message. In this section, we exhibit a constructive way to build these functions. We first exhibit the way to build a generic class of reliable selections inside the protection of the most external key (or simply the external key). Then we propose specialized selections of this class. Finally we give the way to build reliable selection-based interpretation functions. Similar techniques based on selections were proposed in previous works, especially in [8, 10, 11] to build universal functions based on the selection of the direct key of encryption and in [18] to check correspondences in protocols. But first of all, we present the notion of well-protected messages that have valuable properties that we will use in the definition of reliable selections. Briefly, a well-protected message is a message such that every non public atom α in it is encrypted by at least one key k such that $\ulcorner k^{-1} \urcorner \sqsupseteq \ulcorner \alpha \urcorner$, after elimination of unnecessary keys $(\text{e.g. } e(k, d(k^{-1}, m)) \rightarrow m)$. The main advantage of an analysis performed over a set of well-protected messages is that the intruder cannot deduce any secret when she uses only her knowledge in the context of verification (without using the protocol rules).

4.1 Protocol analysis in Well-Protected Messages

We denote by $\mathcal{E}_\mathcal{C}$ the set of encryption functions and by $\overline{\mathcal{E}}_\mathcal{C}$ the complementary set $\Sigma \backslash \mathcal{E}_\mathcal{C}$ in a context of verification $\mathcal{C}$.

The definition 4.1 defines the application $keys$ that returns the encryption keys of any atom α in a message m.

Definition 4.1. (Keys)
Let $M \subseteq \mathcal{M}$, $f \in \Sigma$ and $m \in M$.
We define the application $Keys: \mathcal{A} \times \mathcal{M} \longrightarrow \mathcal{P}(\mathcal{P}(\mathcal{A}))$ as follows:
$\forall t_1, t_2 ... t_n$ subterms of m:

$$\begin{aligned}
&Keys(\alpha, \alpha) && = \{\emptyset\} \\
&Keys(\alpha, \beta) && = \emptyset, \text{ if } \alpha \neq \beta \text{ and } \beta \in \mathcal{A} \\
&Keys(\alpha, f_k(t_1, ..., t_n)) && = \{k\} \otimes \bigcup_{i=1}^{n} Keys(\alpha, t_i), \text{ if } f_k \in \mathcal{E}_\mathcal{C} \\
&Keys(\alpha, f(t_1, ..., t_n)) && = \bigcup_{i=1}^{n} Keys(\alpha, t_i), \text{ if } f \in \overline{\mathcal{E}}_\mathcal{C}
\end{aligned}$$

We extend the application $Keys$ to sets as follows:

$$\forall M \subseteq \mathcal{M}. Keys(\alpha, M) = \bigcup_{m \in M} Keys(\alpha, m) \text{ and } Keys(\alpha, \emptyset) = \emptyset.$$

The definition 4.2 is related to equational theory. It fixes the form of a message that we are going to choose. The chosen form (normal form) is the one that provides the smallest set of encryption keys. This in order to eliminate the unnecessary keys (e.g. $e(k, d(k^{-1}, m)) \rightarrow m$).

Definition 4.2. (Equational theory, Rewriting system and Normal Form)
We assume that we can transform the equational theory ξ given in the context of verification to a convergent rewriting system $\rightarrow_\xi$ such that:

$$\forall m \in \mathcal{M}, \forall \alpha \in \mathcal{A}(m), \forall l \rightarrow r \in \rightarrow_\xi, \qquad Keys(\alpha, r) \subseteq Keys(\alpha, l) \tag{6}$$

We denote by $m_\Downarrow$ the normal form of m in $\rightarrow_\xi$.

The kind of rewriting systems orientation in the definition 4.2 poses no problem with the most of equational theories in the literature [19–21].

Example 4.3.
Let $m = \{\{\{A.\alpha\}_{k_{ab}}\}_{k_{ab}^{-1}}\}_{k_{ac}}$; $m_\Downarrow = \{A.\alpha\}_{k_{ac}}$

In the definition 4.4, we introduce the application $Access$. Every element of $Access(\alpha, m)$ contains a set of required keys to decrypt α in m after elimination of unnecessary keys by the normal form defined in 4.2.

Definition 4.4. (Access)
Let $M \subseteq \mathcal{M}$, $f \in \Sigma$ and $m \in M$.
We define the application $Access : \mathcal{A} \times \mathcal{M} \longrightarrow \mathcal{P}(\mathcal{P}(\mathcal{A}))$ as follows:
$\forall t_1, t_2 ... t_n$ subterms of m:

$$\begin{aligned}
&Access(\alpha, \alpha) && = \{\emptyset\}\\
&Access(\alpha, \beta) && = \emptyset, \text{ if } \alpha \neq \beta \text{ and } \beta \in \mathcal{A}\\
&Access(\alpha, f_k(t_1, ..., t_n)) && = \{k^{-1}\} \otimes \bigcup_{i=1}^{n} Access(\alpha, t_i), \text{ if } f_k \in \mathcal{E}_{\mathcal{C}} \text{ and } f_k(t_1, ..., t_n) = f_k(t_1, ..., t_n)_{\Downarrow}\\
&Access(\alpha, f(t_1, ..., t_n)) && = \bigcup_{i=1}^{n} Access(\alpha, t_i), \text{ if } f \in \overline{\mathcal{E}}_{\mathcal{C}} \text{ and } f_k(t_1, ..., t_n) = f_k(t_1, ..., t_n)_{\Downarrow}\\
&Access(\alpha, f(t_1, ..., t_n)) && = Access(\alpha, f(t_1, ..., t_n)_{\Downarrow}), \text{ if not.}
\end{aligned}$$

We extend the application $Access$ to sets as follows:

$$\forall M \subseteq \mathcal{M}. Access(\alpha, M) = \bigcup_{m \in M} Access(\alpha, m) \text{ and } Access(\alpha, \emptyset) = \emptyset.$$

Example 4.5.
Let m be a message such that: $m = \{\{A.D.\alpha\}_{k_{ab}}.\alpha.\{A.E.\{C.\alpha\}_{k_{ef}}\}_{k_{ab}}\}_{k_{ac}}$;
$Access(\alpha, m) = \{\{k_{ac}^{-1}, k_{ab}^{-1}\}, \{k_{ac}^{-1}\}, \{k_{ac}^{-1}, k_{ab}^{-1}, k_{ef}^{-1}\}\}$.

In the definition 4.6, we define a well-protected message. Informally, a well-protected message is a message such that every non-public atom α in it (such that $\ulcorner\alpha\urcorner \sqsupset \perp$) is encrypted by at least one key k such that $\ulcorner k^{-1}\urcorner \sqsupseteq \ulcorner\alpha\urcorner$ after elimination of unnecessary keys by the normal form given in the definition 4.2.

Definition 4.6. (Well-protected message)
Let $\mathcal{C}$ be context of verification, $m \in \mathcal{M}$, $M \subseteq \mathcal{M}$ and $\alpha \in \mathcal{A}(m)$ such that $\ulcorner\alpha\urcorner \sqsupset \perp$.

We say that α is well-protected in m if:

$$\forall \beta \in Access(\alpha, m).\ulcorner\beta\urcorner \sqsupseteq \ulcorner\alpha\urcorner$$

We say that α is well-protected in M if:

$$\forall m \in M.\alpha \text{ is well-protected in } m$$

We say that m is well-protected in $\mathcal{C}$ if:

$$\forall \alpha \in \mathcal{A}(m).\alpha \text{ is well-protected in } m$$

We say that M is well-protected in $\mathcal{C}$ if:

$$\forall m \in M.m \text{ is well-protected in } \mathcal{C}.$$

In the definition 4.7, we define the application $Clear(m)$. Informally, $Clear(m)$ returns the set of all atoms that appear in clear in m after elimination of unnecessary keys by the normal form given in the definition 4.2.

Definition 4.7. ($Clear$)
Let $m \in \mathcal{M}$ and $M \subset \mathcal{M}$.

$$Clear(m) = \{\alpha \in \mathcal{A}(m).\ \emptyset \in Access(\alpha, m)\}$$

We extend this definition to sets as follows :

$$Clear(M) = \bigcup_{m \in M} Clear(m)$$

Lemma 4.8.
Let M be a set of well-protected messages in $\mathcal{M}$. We have:

$$M \models_{\mathcal{C}} m \Rightarrow \forall \alpha \in \mathcal{A}(m).(\alpha \text{ is well-protected in } m) \vee (\ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner)$$

See the proof 7 in [17]

The lemma 4.8 says that from a set of well-protected messages, all atomic messages beyond the knowledge of the intruder (i.e. $\ulcorner K(I) \urcorner \not\sqsupseteq \ulcorner \alpha \urcorner$) remain well-protected in any message that the intruder could infer. Indeed, since each atom that does not appear in clear (non-public) in this set is encrypted by at least one key k such that $\ulcorner k^{-1} \urcorner \sqsupseteq \ulcorner \alpha \urcorner$, then the intruder has to retrieve the key k^{-1} before she sees α not well-protected in any message (clear). But, the key k^{-1} is in its turn encrypted by at least one key k' such that $\ulcorner k'^{-1} \urcorner \sqsupseteq \ulcorner k^{-1} \urcorner$. The proof is then conducted by induction on the encryption keys.

Lemma 4.9. (Lemma of non-disclosure of atomic secrets in well-protected messages)
Let M be a set of well-protected messages in $\mathcal{M}$ and α an atomic message in M.
We have:

$$M \models_{\mathcal{C}} \alpha \Rightarrow \ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner$$

Proof.

From the lemma 4.8, we have $M \models_{\mathcal{C}} \alpha$ then:

$$(\alpha \text{ is well-protected in } \alpha) \vee (\ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner) \quad (7)$$

But α is not well-protected in α, then we have:

$$\ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner \quad (8)$$

4.2 Discussion and Assumption

The lemma 4.9 expresses an important result. It states that from a set of well-protected messages the intruder cannot deduce any secret that she is not supposed to know when she uses only her knowledge in the context of verification (without using the protocol rules). It is worth saying that verifying whether a protocol operates over a space of well-protected messages or not is an easy task and most of real protocols respect this condition.

4.3 Building reliable selections

Now, we will focus on building selections such that when they are composed to suitable homomorphisms, provide reliable interpretation functions. The definition 4.10 introduces the notion of a well-formed selection and the definition 4.11 introduces the notion of a full-invariant-by-intruder selection**.**

Definition 4.10. (Well-formed selection)
Let $M, M_1, M_2 \subseteq \mathcal{M}$ such that M, M_1 and M_2 are well-protected.

Let $S : \mathcal{A} \times \mathcal{M} \longmapsto 2^{\mathcal{A}}$ be a selection.
We say that S is well-formed in $\mathcal{C}$ if:

$$\begin{cases} S(\alpha, \{\alpha\}) & = & \mathcal{A}, \\ S(\alpha, M_1 \cup M_2) & = & S(\alpha, M_1) \cup S(\alpha, M_2), \\ S(\alpha, M) & = & \emptyset, \text{if } \alpha \notin \mathcal{A}(M) \end{cases}$$

For an atom α in a set of messages M, a well-formed selection returns all the atoms in $\mathcal{M}$ if $M = \{\alpha\}$. It returns for it in the union of two sets of messages, the union of the two selections performed in each set separately. It returns the empty set if the atom does not appear in M.

Definition 4.11. (Full-invariant-by-intruder selection)
Let $M \subseteq \mathcal{M}$ such that M is well-protected.
Let $S : \mathcal{A} \times \mathcal{M} \longmapsto 2^{\mathcal{A}}$ be a selection.
We say that S is full-invariant-by-intruder in $\mathcal{C}$ if:
$\forall M \subseteq \mathcal{M}, m \in \mathcal{M}$, we have:

$$M \models_{\mathcal{C}} m \Rightarrow \forall \alpha \in \mathcal{A}(m).(S(\alpha, m) \subseteq S(\alpha, M)) \vee (\ulcorner K(I) \urcorner \sqsupseteq \ulcorner \alpha \urcorner)$$

The aim of a full-invariant-by-intruder selection is to provide a full-invariant-by-intruder function when composed to an adequate homomorphism that transforms its returned atoms into security levels. Since a full-invariant-by-intruder function is requested to resist to any attempt of the intruder to generate a message m from any set of messages M in which the level of security of an atom, that she is not allowed to know, decreases compared to it its value in M, a full-invariant-by-intruder selection is requested to resist to any attempt of the intruder to generate a message m from any set of messages M in which the selection associated to an atom, that she is not allowed to know, could be enlarged compared to the selection associated to this atom in M. This fact is described by the definition 4.11.

Definition 4.12. (Reliable selection)
Let $S : \mathcal{A} \times \mathcal{M} \longmapsto 2^{\mathcal{A}}$ be a selection and $\mathcal{C}$ be a context of verification.

S is $\mathcal{C}$-reliable if S is well-formed and S is full-invariant-by-intruder in $\mathcal{C}$.

4.3.1 Reliable selections inside the protection of an external key

Here, we define a generic class of selections that we denote by S^{EK}_{Gen} and we prove that any instance of it is reliable under some condition.

Definition 4.13. (S^{EK}_{Gen}: selection inside the protection of an external key)
We denote by S^{EK}_{Gen} the class of all selections S that meet the following conditions:

- $S(\alpha, \alpha) = \mathcal{A}$; (9)
- $S(\alpha, m) = \emptyset$, if $\alpha \notin \mathcal{A}(m)$; (10)
- $\forall \alpha \in \mathcal{A}(m)$, where $m = f_k(m_1, ..., m_n)$:

$$S(\alpha, m) \subseteq (\underset{1 \leq i \leq n}{\cup} \mathcal{A}(m_i) \cup \{k^{-1}\} \backslash \{\alpha\}) \text{ if } f_k \in \mathcal{E}_{\mathcal{C}} \text{ and } \ulcorner k^{-1} \urcorner \sqsupseteq \ulcorner \alpha \urcorner \text{ and } m = m_{\Downarrow} \quad (11)$$

- $\forall \alpha \in \mathcal{A}(m)$, where $m = f(m_1, ..., m_n)$:

$$S(\alpha, m) = \begin{cases} \underset{1 \leq i \leq n}{\cup} S(\alpha, m_i) & \text{if } f_k \in \mathcal{E}_{\mathcal{C}} \text{ and } \ulcorner k^{-1} \urcorner \not\sqsupseteq \ulcorner \alpha \urcorner \text{ and } m = m_{\Downarrow} \text{ (a)} \\ \underset{1 \leq i \leq n}{\cup} S(\alpha, m_i) & \text{if } f \in \overline{\mathcal{E}}_{\mathcal{C}} \text{ and } m = m_{\Downarrow} \text{ (b)} \\ S(\alpha, m_{\Downarrow}) & \text{if } m \neq m_{\Downarrow} \text{ (c)} \end{cases} \quad (12)$$

- $S(\alpha, \{m\} \cup M) = S(\alpha, m) \cup S(\alpha, M)$ (13)

For an atom α in an encrypted message $m = f_k(m_1, ..., m_n)$, a selection S as defined above returns a subset (see "$\subseteq$" in equation 11) among atoms that are neighbors of α in m inside the protection of the most external protective key k including its reverse form k^{-1}. The atom α itself is not selected. This set of candidate atoms is denoted by $\underset{1 \leq i \leq n}{\cup} \mathcal{A}(m_i) \cup \{k^{-1}\} \backslash \{\alpha\}$ in the equation 11. The most external protective key (or simply the external key) is the most external one that satisfies $\ulcorner k^{-1} \urcorner \sqsupseteq \ulcorner \alpha \urcorner$. A such key must exist when the set of messages generated by the protocol is well-protected, which is one of our assumptions above. By neighbor of α in m, we mean any atom that travels with it inside the protection of the external key.

S^{EK}_{Gen} defines a generic class of selections since it does not identify what atoms to select precisely inside the protection of the external key. It identifies only the atoms that are candidates for selection and among them we are allowed to return any subset.

Proposition 4.14.
Let $S \in S^{EK}_{Gen}$ and $\mathcal{C}$ be a context of verification.
Let's have a rewriting system $\rightarrow_{\xi}$ such that $\forall m \in \mathcal{M}, \forall \alpha \in \mathcal{A}(m) \wedge \alpha \notin Clear(m)$, we have:

$$\forall l \rightarrow r \in \rightarrow_{\xi}, S(\alpha, r) \subseteq S(\alpha, l) \quad (14)$$

We have:

S is $\mathcal{C}$-reliable.

See the proof 11 in [17]

Remark. The condition on the rewriting system $\rightarrow_{\xi}$ given by the equation 14 in the definition 4.14 is introduced to make sure that the selection in the normal form is the smallest among all forms of a given message. This prevents the selection S to select atoms that are inserted maliciously by the intruder by manipulating the equational theory. Hence, we are sure that all selected atoms by S are honest. For example, let $m = \{\alpha.S\}_{k_{ab}}$ be a message in a homomorphic cryptography (i.e $\{\alpha.S\}_{k_{ab}} = \{\alpha\}_{k_{ab}}.\{S\}_{k_{ab}}$). In the form $\{\alpha.S\}_{k_{ab}}$, the selection $S(\alpha, \{\alpha.S\}_{k_{ab}})$ may select S since S is a neighbor of α inside the protection of k_{ab}, but in the

form $\{\alpha\}_{k_{ab}}.\{S\}_{k_{ab}}$ the selection $S(\alpha, \{\alpha\}_{k_{ab}}.\{S\}_{k_{ab}})$ may not because it is not a neighbor of α. Then, we must make sure that the rewriting system $\rightarrow_\xi$ we are using is oriented in such way that it chooses the form $\{\alpha\}_{k_{ab}}.\{S\}_{k_{ab}}$ rather than the form $\{\alpha.S\}_{k_{ab}}$ because there is no guarantee that S is a honest neighbor and that it had not been inserted maliciously by the intruder using the homomorphic property in the theory. We assume that the rewriting system we are using meets this condition.

For the proposition 4.14, it is easy to check that by constuction a selection S, that is instance of S^{EK}_{Gen}, is well-formed. The proof of full-invariance-by-intruder is carried out by induction on the tree of construction of a message. The principal idea of the proof is that the selection related to an atom α in a message m takes place inside the encryption by the most external protective key (such that: $\ulcorner k^{-1} \urcorner \sqsupseteq \ulcorner \alpha \urcorner$). Thus an intruder cannot modify this selection when she does not have the key k^{-1} (i.e. $\ulcorner K(I) \urcorner \not\sqsupseteq \ulcorner k^{-1} \urcorner$). Besides, according to the lemma 4.9, in a set of well-protected messages the intruder can never infer this key since it is atomic. So, this selection can only be modified by people who are initially authorized to know α (i.e $\ulcorner K \urcorner \sqsupseteq \ulcorner k^{-1} \urcorner$ and then $\ulcorner K \urcorner \sqsupseteq \ulcorner \alpha \urcorner$) In addition, the intruder cannot neither use the equational theory to alter this selection thanks to the condition made on the rewriting system in the remark 4.3.1. Therefore any set of candidate atoms returned by S cannot be altered (enlarged) by the intruder in any message m that she can infer, as required by a full-invariant-by-intruder selection.

Example 4.15.
Let α be an atomic message and m a message such that: $\ulcorner \alpha \urcorner = \{A, B\}$ and $m = \{A.C.\alpha.D\}_{k_{ab}}$. Let S_1, S_2 and S_3 be three selections such that: $S_1(\alpha, m) = \{k_{ab}^{-1}\}$, $S_2(\alpha, m) = \{A, C, k_{ab}^{-1}\}$ and $S_3(\alpha, m) = \{A, C, D, k_{ab}^{-1}\}$. These three selections are $\mathcal{C}$-reliable.

4.4 Instantiation of reliable selections from the class S^{EK}_{Gen}

Now that we defined a generic class of reliable selections S^{EK}_{Gen}, we will instantiate some concrete selections from it, that are naturally reliable. Instantiating S^{EK}_{Gen} consists in defining selections that return precise sets of atoms among the candidates allowed by S^{EK}_{Gen}.

4.4.1 The selection S^{EK}_{MAX}
The selection S^{EK}_{MAX} is the instance of the class S^{EK}_{Gen} that returns for an atom in a message m all its neighbors, that are principal identities, inside the protection of the external protective key k in addition to its reverse key k^{-1}. (MAX means: the MAXimum of principal identities)

4.4.2 The selection S^{EK}_{EK}
The selection S^{EK}_{EK} is the instance of the class S^{EK}_{Gen} that returns for an atom in a message m only the reverse key of the external protective key. (EK means: External Key)

4.4.3 The selection S^{EK}_{N}
The selection S^{EK}_{N} is the instance of the class S^{EK}_{Gen} that returns only its neighbors, that are principal identities, inside the protection of the external protective key. (N means: Neighbors)

Example 4.16.
Let α be an atom and m a message such that: $\ulcorner\alpha\urcorner = \{A, C\}$ and $m = \{\{\{\alpha.E\}_{k_{ab}}.F\}_{k_{ac}}.D\}_{k_{ad}}$
$S^{EK}_{MAX}(\alpha, m) = \{E, F, k^{-1}_{ac}\}$; $S^{EK}_{EK}(\alpha, m) = \{k^{-1}_{ac}\}$; $S^{EK}_{N}(\alpha, m) = \{E, F\}$

4.5 Specialized C-reliable selection-based interpretation functions

Now, we define specific functions that are a composition of an appropriate homomorphism and instances of the class of selections S^{EK}_{Gen}. This homomorphism exports the properties of reliability from a selection to a function and transforms selected atoms to security levels. The following proposition states that any function that is a composition of the homomorphism defined below and the selections S^{EK}_{Gen} is reliable.

Proposition 4.17.
Let ψ be a homomorphism defined as follows:

$$\begin{array}{rcccl} \psi & : & (2^{\mathcal{A}})^{\subseteq} & \mapsto & \mathcal{L}^{\sqsupseteq} \\ & & M & \mapsto & \begin{cases} \top & \text{if } M = \emptyset \\ \sqcap_{\alpha \in M} \psi(\alpha) & \text{if not.} \end{cases} \end{array}$$

$$\text{such that: } \psi(\alpha) = \begin{cases} \{\alpha\} & \text{if } \alpha \in \mathcal{I} \text{ (Principal Identities)} \\ \ulcorner\alpha\urcorner & \text{if not.} \end{cases}$$

We have: $F^{EK}_{MAX} = \psi \circ S^{EK}_{MAX}$, $F^{EK}_{EK} = \psi \circ S^{EK}_{EK}$ and $F^{EK}_{N} = \psi \circ S^{EK}_{N}$ are $\mathcal{C}$-reliable.

See the proof 17 in [17]

The homomorphism ψ in the proposition 4.17 assigns for a principal in a selection, its identity. It assigns for a key its level of security in the context of verification. This homomorphism ensures the mapping from the operator "$\subseteq$" to the operator "$\sqsupseteq$" in the lattice which offers to an interpretation function to inherit the full-invariance-by-intruder from its associated selection. In addition, it ensures the mapping from the operator "$\cup$" to the operator "$\sqcap$" in the lattice, which offers to an interpretation function to be well-formed if its associated selection is well-formed. Generally, every function $\psi \circ S$ remains reliable for any selection S in S^{EK}_{Gen}.

Example 4.18.
Let α be an atom, m a message and k_{ab} a key such that:
$\ulcorner\alpha\urcorner = \{A, B, S\}$; $m = \{A.C.\alpha.D\}_{k_{ab}}$; $\ulcorner k^{-1}_{ab}\urcorner = \{A, B, S\}$;
$S^{EK}_{EK}(\alpha, m) = \{k^{-1}_{ab}\}$; $S^{EK}_{N}(\alpha, m) = \{A, C, D\}$; $S^{EK}_{MAX}(\alpha, m) = \{A, C, D, k^{-1}_{ab}\}$;
$F^{EK}_{EK}(\alpha, m) = \psi \circ S^{EK}_{EK}(\alpha, m) = \ulcorner k^{-1}_{ab}\urcorner = \{A, B, S\}$; $F^{EK}_{N}(\alpha, m) = \psi \circ S^{EK}_{N}(\alpha, m) = \{A, C, D\}$;
$F^{EK}_{MAX}(\alpha, m) = \psi \circ S^{EK}_{MAX}(\alpha, m) = \{A, C, D\} \cup \ulcorner k^{-1}_{ab}\urcorner = \{A, C, D\} \cup \{A, B, S\} = \{A, C, D, B, S\}$.

5. INSUFFICIENCY OF RELIABLE INTERPRETATION FUNCTIONS TO ANALYZE GENERALIZED ROLES

So far, we presented a class of selection-based interpretation functions that have the required properties to analyze protocols statically. Unfortunatly, they operate on valid traces that contain closed messages only. Nevertheless, a static analysis must be led over the finite set of messages

of the generalized roles of the protocol because the set of valid traces is infinite. The problem is that the finite set of the generalized roles contains variables and the functions we defined are not "enough prepared" to analyze such messages because they are not supposed to be full-invariant by substitution [22–24]. The full-invariance by substitution is the property that allows us to perform an analysis over messages with variables and to export the conclusion made-on to closed messages. In the following section, we deal with the substitution question. We introduce the concept of derivative messages to reduce the impact of variables and we build the witness functions that operate on these derivative messages rather than messages themselves. As we will see, the witness-functions provide two interesting bounds that are independent of all substitutions. This fully replaces the property of full-invariance by substitution. Finally, we define a criterion of protocol correctness based on these two bounds.

5.1 Derivative message

Let $m, m_1, m_2 \in \mathcal{M}$; $\mathcal{X}_m = Var(m)$; $S_1, S_2 \subseteq 2^{\mathcal{X}_m}$; $\alpha \in \mathcal{A}(m)$; $X, Y \in \mathcal{X}_m$ and ϵ be the empty message.

Definition 5.1. (Derivation)
We define the derivative message as follows:

$$\begin{array}{ll}
\partial_X \epsilon & = \epsilon \\
\partial_X \alpha & = \alpha \\
\partial_X X & = \epsilon \\
\partial_X Y & = Y, X \neq Y \\
\partial_X f(m) & = f(\partial_X m), f \in \mathcal{E}_\mathcal{C} \cup \overline{\mathcal{E}}_\mathcal{C} \\
\partial_{\{X\}} m & = \partial_X m \\
\partial_{(\overline{X})} m & = \partial_{\{\mathcal{X}_m \setminus X\}} m \\
\partial_{S_1 \cup S_2} m & = \partial_{S_2 \cup S_1} m = \partial_{S_1} \partial_{S_2} m = \partial_{S_2} \partial_{S_1} m
\end{array}$$

To be simple, we denote by ∂m the expression $\partial_{\mathcal{X}_m} m$. The operation of derivation introduced by the definition 5.1 (denoted by ∂) eliminates variables in a message. $\partial_X m$ consists in eliminating the variable X in m. $\partial(\overline{X})m$ consists in eliminating all variables, except X, in m. Hence, X when overlined is considered as a constant in m. ∂m consists in eliminating all the variables in m.

Definition 5.2.
Let $m \in \mathcal{M}_p^\mathcal{G}$, $X \in \mathcal{X}_m$ and $m\sigma$ be a closed message.
For all $\alpha \in \mathcal{A}(m\sigma)$, $\sigma \in \Gamma$, we denote by:

$$F(\alpha, \partial[\overline{\alpha}]m\sigma) = \begin{cases} \top & \text{if } \alpha \notin \mathcal{A}(m\sigma), \\ F(\alpha, \partial m) & \text{if } \alpha \in \mathcal{A}(\partial m), \\ F(X, \partial[\overline{X}]m) & \text{if } \alpha \in \mathcal{A}(X\sigma) \wedge \alpha \notin \mathcal{A}(\partial m). \end{cases}$$

A message m in a generalized role is composed of two parts: a static part and a dynamic part. The dynamic part is described by variables. For an atom α in the static part (i.e. ∂m), $F(\alpha, \partial[\overline{\alpha}]m\sigma)$ removes the variables in m and gives it the value $F(\alpha, \partial m)$. For anything that is not an atom of the static part -that comes by substitution of some variable X in m- $F(\alpha, \partial[\overline{\alpha}]m\sigma)$ considers it as the variable itself, treated as a constant and as a block, and gives it all the time the same value: $F(X, \partial[\overline{X}]m)$. It gives the top value for any atom that does

not appear in $m\sigma$. For any F such that its associated selection is an instance of the class S^{EK}_{Gen}, $F(\alpha, \partial[\overline{\alpha}]m\sigma)$depends only on the static part of m since α is not selected. The function in the definition 5.2 presents the three following major facts :

1. An atom of the static part of a message with variables, when analyzed with a such function, is considered as an atom in a message with no variables (a closed message);
2. A variable, when analyzed by such function, is considered as any component that substitutes it (that is not in the static part of the message) with no respect to other variables, if any;
3. For any F such that its associated selection is an instance of the class S^{EK}_{Gen}, $F(\alpha, \partial[\overline{\alpha}]m\sigma)$ depends only on the static part of m since α is not selected.

One could suggest that we attribute to an atom α in a closed message mσ the value returned by the function $F(\alpha, \partial[\overline{\alpha}]m\sigma)$ given in the definition 5.2 and hence we neutralize the variable effects. Unfortunately, this does not happen without undesirable "side-effects" because derivation generates a "loss of details". Let's look at the example 5.3.

Example 5.3.
Let m_1 and m_2 be two messages of a generalized role of a protocol p such that $m_1 = \{\alpha.C.X\}_{k_{ab}}$ and $m_2 = \{\alpha.Y.D\}_{k_{ab}}$ and $\ulcorner\alpha\urcorner = \{A, B\}$;
Let $m = \{\alpha.C.D\}_{k_{as}}$ be a closed message in a valid trace generated by p;

$$F^{EK}_{MAX}(\alpha, \partial[\overline{\alpha}]m) = \begin{cases} \{C, A, B\} & \text{if } m \text{ comes by the substitution of } X \text{ by } D \text{ in } m_1 \\ \{D, A, B\} & \text{if } m \text{ comes by the substitution of } Y \text{ by } C \text{ in } m_2 \end{cases}$$

Hence $F^{EK}_{MAX}(\alpha, \partial[\overline{\alpha}]m)$ is not even a function on the closed message m since it may return more than one image for the same preimage. This leads us straightly to the witness-functions.

6. THE WITNESS-FUNCTIONS

Definition 6.1. (Witness-Function)
Let $m \in \mathcal{M}^{\mathcal{G}}_p$, $X \in \mathcal{X}_m$ and $m\sigma$ be a closed message.
Let p be a protocol and F be a $\mathcal{C}$-reliable interpretation function.
We define a witness-function $\mathcal{W}_{p,F}$ for all $\alpha \in \mathcal{A}(m\sigma)$, $\sigma \in \Gamma$, as follows:

$$\mathcal{W}_{p,F}(\alpha, m\sigma) = \bigsqcap_{\substack{m' \in \mathcal{M}^{\mathcal{G}}_p \\ \exists \sigma' \in \Gamma . m'\sigma' = m\sigma}} F(\alpha, \partial[\overline{\alpha}]m'\sigma')$$

$\mathcal{W}_{p,F}$ is said a witness-function inside the protection of an external key when F is an interpretation function such that its associated selection is an instance of the class S^{EK}_{Gen}.

According to the example 5.3, the application defined in 5.2 is not necessary a function in $\mathcal{M}_p^{\mathcal{G}}$ as a valid trace could have more than one source (or provenance) in $\mathcal{M}_p^{\mathcal{G}}$ and each source has a different static part. A witness-function is yet a function in p since it searches all the sources of the closed message in input and returns the minimum (the union). This minimum naturally exists and is unique in the finite set $\mathcal{M}_p^{\mathcal{G}}$. A witness-function is protocol-dependent as it depends on messages in the generalized roles of the protocol. However, it is built uniformly for any pair (protocol, interpretation function) in input.

Remark.

For a witness-function inside the protection of an external key, since its associated interpretation function ranks an atom always from a message m having an encryption pattern, i.e. when $f_k \in \mathcal{E}_{\mathcal{C}}$, the search of the sources of the closed message $m\sigma$ in $\mathcal{M}_p^{\mathcal{G}}$ (i.e. $\{m' \in \mathcal{M}_p^{\mathcal{G}} | \exists \sigma' \in \Gamma . m'\sigma' = m\sigma\}$) is limited to a search in the encryption patterns in $\mathcal{M}_p^{\mathcal{G}}$.

6.1 Legacy of Reliability

The proposition 6.2 asserts that an interpretation function F inside the protection of an external key transmits its reliability to its associated witness-function $\mathcal{W}_{p,F}$. In fact, the selection associated with a witness function inside the protection of an external key is the union of selections associated with the interpretation function F, limited to derivative messages. It is easy to check that a witness-function is well-formed. Concerning the full-invariance-by-intruder property, as the derivation just eliminates variables (so some atoms when the message is substituted), and since each selection in the union returns a subset among allowed candidates, then the union itself returns a subset among allowed candidates (the union of subsets is a subset). Therefore, the selection associated with a witness-function stays an instance of the class S_{Gen}^{EK}, so full-invariant-by-intruder. Since the witness-function is the composition of the homomorphism of F and an instance of the class S_{Gen}^{EK}, then it is reliable.

Proposition 6.2.

Let $\mathcal{W}_{p,F}$ be a witness-function inside the protection of an external key.
We have:

$\mathcal{W}_{p,F}$ inherits reliability from F.

See the proof 18 in [17]

6.2 Bounds of a Witness-Function

In the lemma 6.4, we define two interresting bounds of a witness-function that are independent of all substitutions. The upper bound of a witness-function ranks the security level of an atom α in a closed message mσ from one confirmed source m (m is a natural source of mσ), the witness-function itself ranks it from the exact sources of mσ that are known only when the protocol is run, and the lower bound ranks it from the exact sources of mσ that are known only when the protocol is run, and the lower bound ranks it from all likely sources of mσ (i.e. the messages that are unifiable with m in $\mathcal{M}_p^{\mathcal{G}}$).

Example 6.3.
Let $\mathcal{M}_p^{\mathcal{G}} = \{\{\alpha.B.X\}_{k_{ad}}, \{\alpha.Y.S\}_{k_{ad}}, \{A.Z\}_{k_{bc}}\}$ with $Var(\mathcal{M}_p^{\mathcal{G}}) = \{X, Y, Z\}$;
Let $m_1 = \{\alpha.B.S\}_{k_{ad}}$; $m_2 = \{A.\gamma\}_{k_{bc}}$; $\ulcorner\alpha\urcorner = \{A, D\}$; $\ulcorner k_{ad}^{-1}\urcorner = \{A, D\}$; $\ulcorner k_{bc}^{-1}\urcorner = \{B, C\}$;
• $\mathcal{W}_{p,F_{MAX}^{EK}}(\alpha, m_1)$
= {Definition 6.1}
$\sqcap_{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = m_1}} F_{MAX}^{EK}(\alpha, \partial[\overline{\alpha}]m'\sigma') = \sqcap_{\substack{\{\{\alpha.B.X\}_{k_{ad}}, \{\alpha.Y.S\}_{k_{ad}}\} \\ \sigma' = \{X \longmapsto S, Y \longmapsto B\}}} F_{MAX}^{EK}(\alpha, \partial[\overline{\alpha}]m'\sigma')$
= {$\mathcal{W}_{p,F_{MAX}^{EK}}$ is well-formed from the proposition 6.2}
$F_{MAX}^{EK}(\alpha, \partial[\overline{\alpha}]\{\alpha.B.X\}_{k_{ad}}[X \longmapsto S]) \sqcap F_{MAX}^{EK}(\alpha, \partial[\overline{\alpha}]\{\alpha.Y.S\}_{k_{ad}}[Y \longmapsto B])$
= {Definition 5.2 and derivation in 5.1}
$F_{MAX}^{EK}(\alpha, \{\alpha.B\}_{k_{ad}}) \sqcap F_{MAX}^{EK}(\alpha, \{\alpha.S\}_{k_{ad}})$
= {Definition of F_{MAX}^{EK}}
$\{B, A, D\} \cup \{S, A, D\} = \{B, A, D, S\}$
• $\mathcal{W}_{p,F_{MAX}^{EK}}(\gamma, m_2)$
= {Definition 6.1}
$\sqcap_{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = m_2}} F_{MAX}^{EK}(\gamma, \partial[\overline{\gamma}]m'\sigma') = \sqcap_{\substack{\{\{A.Z\}_{k_{bc}}\} \\ \sigma' = \{Z \longmapsto \gamma\}}} F_{MAX}^{EK}(\gamma, \partial[\overline{\gamma}]m'\sigma') =$
$F_{MAX}^{EK}(\gamma, \partial[\overline{\gamma}]\{A.Z\}_{k_{bc}}[Z \longmapsto \gamma])$
= {Definition 5.2}
$F_{MAX}^{EK}(Z, \partial[\overline{Z}]\{A.Z\}_{k_{bc}})$
= {Derivation in 5.1 }
$F_{MAX}^{EK}(Z, \{A.Z\}_{k_{bc}})$
= {Definition of F_{MAX}^{EK}}
$\{A, B, C\}$

Lemma 6.4.
Let $m \in \mathcal{M}_p^{\mathcal{G}}$ and $\mathcal{W}_{p,F}$ be a witness-function inside the protection of an external key.
$\forall \sigma \in \Gamma, \forall \alpha \in \mathcal{A}(\mathcal{M}_p)$ we have:

$$F(\alpha, \partial[\overline{\alpha}]m) \sqsupseteq \mathcal{W}_{p,F}(\alpha, m\sigma) \sqsupseteq \sqcap_{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = m\sigma'}} F(\alpha, \partial[\overline{\alpha}]m'\sigma')$$

Proof.
For any $\sigma \in \Gamma$ we have:

- $F(\alpha, \partial[\overline{\alpha}]m) \subseteq \mathcal{W}_{p,F}(\alpha, m\sigma)$: since m is obviously one element of the set $\{m' \in \mathcal{M}_p^{\mathcal{G}} | \exists \sigma' \in \Gamma. m'\sigma' = m\sigma\}$ of calculation of $\mathcal{W}_{p,F}(\alpha, m\sigma)$ (i.e. m is a trivial source of $m\sigma$) and since $F(\alpha, \partial[\overline{\alpha}]m\sigma)$ does not depend on σ because, by construction, it depends only on the static part of m (denoted simply by $F(\alpha, \partial[\overline{\alpha}]m)$).
- $\mathcal{W}_{p,F}(\alpha, m\sigma) \subseteq \cup_{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = m\sigma'}} F(\alpha, \partial[\overline{\alpha}]m'\sigma')$: since for all $m \in \mathcal{M}_p^{\mathcal{G}}$ the set $\{m' \in \mathcal{M}_p^{\mathcal{G}} | \exists \sigma' \in \Gamma. m'\sigma' = m\sigma'\}$ (unifications) is obviously larger than the set $\{m' \in \mathcal{M}_p^{\mathcal{G}} | \exists \sigma' \in \Gamma. m'\sigma' = m\sigma\}$ of sources of $m\sigma$ in $\mathcal{M}_p^{\mathcal{G}}$.

From these two facts and since $\mathcal{L}^{\sqsupseteq}$ is a lattice, we have the result in the lemma 6.4

6.3 Protocol correctness with a Witness-Function Theorem

Now, we give the protocol analysis with a Witness-Function theorem that sets a criterion for protocols correctness with respect to the secrecy property. The result in the theorem 6.5 derives directly from the proposition 6.2, the lemma 6.4 and the theorem 3.7. The independence of the criterion stated by the theorem 6.5 of all substitutions fully replaces the condition of full-invariance by substitution stated in Houmani's work [8, 11], and hence any decision made on the generalized roles could be propagated to valid traces.

Theorem 6.5. (Protocol analysis with a Witness-Function)
Let $\mathcal{W}_{p,F}$ be a witness-function inside the protection of an external key.
A sufficient condition of correctness of p with respect to the secrecy property is:
$\forall R.r \in R_G(p), \forall \alpha \in \mathcal{A}(r^+)$ we have:

$$\sqcap_{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = r^+\sigma'}} F(\alpha, \partial[\overline{\alpha}]m'\sigma') \sqsupseteq \ulcorner \alpha \urcorner \sqcap F(\alpha, \partial[\overline{\alpha}]R^-)$$

Proof.
Suppose we have: $\forall R.r \in R_G(p), \forall \alpha \in \mathcal{A}(r^+)$

$$\sqcap_{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = r^+\sigma'}} F(\alpha, \partial[\overline{\alpha}]m'\sigma') \sqsupseteq \ulcorner \alpha \urcorner \sqcap F(\alpha, \partial[\overline{\alpha}]R^-) \quad (15)$$

From the lemma 6.4 and since $\mathcal{L}^{\sqsupseteq}$ is a lattice we have for all $\sigma \in \Gamma$:

$$\forall \alpha \in \mathcal{A}(\mathcal{M}_p). \mathcal{W}_{p,F}(\alpha, r^+\sigma) \sqsupseteq \sqcap_{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = r^+\sigma'}} F(\alpha, \partial[\overline{\alpha}]m'\sigma') \quad (16)$$

and

$$\forall \alpha \in \mathcal{A}(\mathcal{M}_p). \ulcorner \alpha \urcorner \sqcap F(\alpha, \partial[\overline{\alpha}]R^-) \sqsupseteq \ulcorner \alpha \urcorner \sqcap \mathcal{W}_{p,F}(\alpha, R^-\sigma) \quad (17)$$

From 15, 16 and 17 we have:

$$\forall \alpha \in \mathcal{A}(r^+\sigma). \mathcal{W}_{p,F}(\alpha, r^+\sigma) \sqsupseteq \ulcorner \alpha \urcorner \sqcap \mathcal{W}_{p,F}(\alpha, R^-\sigma) \quad (18)$$

From the proposition 6.2 $\mathcal{W}_{p,F}$ is $\mathcal{C}$-reliable, then we have from the theorem 3.1 and 18:

p is correct with respect to the secrecy property

7. NSL PROTOCOL ANALYSIS WITH A WITNESS-FUNCTION

In this section, we analyze the NSL protocol with a witness-function. First, let's recall it:

$$\begin{array}{lllll} m_1: & A & \longrightarrow & B: & \{N_a.A\}_{k_b} \\ m_2: & B & \longrightarrow & A: & \{B.N_a\}_{k_a}.\{B.N_b\}_{k_a} \\ m_3: & A & \longrightarrow & B: & A.B.\{N_b\}_{k_b} \end{array}$$

The generalized roles of NSL protocol in a role-based specification are $\mathcal{R}_{\mathcal{G}}(p_{NSL}) = \{A^1_{\mathcal{G}}, A^2_{\mathcal{G}}, B^1_{\mathcal{G}}, B^2_{\mathcal{G}}\}$ where:

$$\begin{array}{lllll} A^1_{\mathcal{G}} = & i.1 \quad A & \longrightarrow I(B) & : & \{N^i_a.A\}_{k_b} \\ A^2_{\mathcal{G}} = & i.1 \quad A & \longrightarrow I(B) & : & \{N^i_a.A\}_{k_b} \\ & i.2 \quad I(B) & \longrightarrow A & : & \{B.N^i_a\}_{k_a}.\{B.X\}_{k_a} \\ & i.3 \quad A & \longrightarrow I(B) & : & A.B.\{X\}_{k_b} \\ \\ B^1_{\mathcal{G}} = & i.1 \quad I(A) & \longrightarrow B & : & \{Y.A\}_{k_b} \\ & i.2 \quad B & \longrightarrow I(A) & : & \{B.Y\}_{k_a}.\{B.N^i_b\}_{k_a} \\ B^2_{\mathcal{G}} = & i.1 \quad I(A) & \longrightarrow B & : & \{Y.A\}_{k_b} \\ & i.2 \quad B & \longrightarrow I(A) & : & \{B.Y\}_{k_a}.\{B.N^i_b\}_{k_a} \\ & i.3 \quad I(A) & \longrightarrow B & : & A.B.\{N^i_b\}_{k_b} \end{array}$$

Let's have a context of verification such that: $\ulcorner A \urcorner = \bot$; $\ulcorner B \urcorner = \bot$; $\ulcorner N_a^i \urcorner = \{A, B\}$; $\ulcorner N_b^i \urcorner = \{A, B\}$; $\ulcorner k_a^{-1} \urcorner = \{A\}$; $\ulcorner k_b^{-1} \urcorner = \{B\}$; $(\mathcal{L}, \sqsupseteq, \sqcup, \sqcap, \bot, \top) = (2^{\mathcal{I}}, \subseteq, \cap, \cup, \mathcal{I}, \emptyset)$; $\mathcal{I} = \{I, A, B, A_1, A_2, B_1, B_2, ...\}$;
The set of messages generated by the protocol is $\mathcal{M}_p^{\mathcal{G}} = \{\{N_{A_1}.A_1\}_{k_{B_1}}, \{B_2.N_{A_2}\}_{k_{A_2}}, \{B_3.X_1\}_{k_{A_3}}, \{X_2\}_{k_{B_4}}, \{Y_1.A_4\}_{k_{B_5}}, \{B_6.Y_2\}_{k_{A_5}}, \{B_7.N_{B_7}\}_{k_{A_6}}, \{N_{B_8}\}_{k_{B_8}}\}$
The variables are denoted by X_1, X_2, Y_1 and Y_2;
The static names are denoted by N_{A_1}, A_1, k_{B_1}, B_2, N_{A_2}, k_{A_2}, B_3, k_{A_3}, k_{B_4}, A_4, k_{B_5}, B_6, k_{A_5}, B_7, N_{B_7}, k_{A_6}, N_{B_8} and k_{B_8}.
After the elimination of duplicates, $\mathcal{M}_p^{\mathcal{G}} = \{\{N_{A_1}.A_1\}_{k_{B_1}}, \{B_2.N_{A_2}\}_{k_{A_2}}, \{B_3.X_1\}_{k_{A_3}}, \{X_2\}_{k_{B_4}}, \{Y_1.A_4\}_{k_{B_5}}, \{B_7.N_{B_7}\}_{k_{A_6}}, \{N_{B_8}\}_{k_{B_8}}\}$
Let's select the Witness-Function as follows:
$p = NSL$; $F = F_{MAX}^{EK}$; $\mathcal{W}_{p,F}(\alpha, m\sigma) = \underset{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = m\sigma}}{\sqcap} F(\alpha, \partial[\overline{\alpha}]m'\sigma')$;

Let's denote the lower bound of the Witness-Function by:

$$\mathcal{W}'_{p,F}(\alpha, r^+) = \underset{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = r^+\sigma'}}{\sqcap} F(\alpha, \partial[\overline{\alpha}]m'\sigma')$$

7.1 Results and Interpretation

The results of analysis of the NSL protocol are summarized in the table 2. We notice from the Table 2 that

α	Role	R^-	r^+	$\mathcal{W}'_{p,F}(\alpha, r^+)$	$\ulcorner \alpha \urcorner$	$F(\alpha, \partial[\overline{\alpha}]R^-)$	Theorem 6.5
N_a^i	A	$\emptyset$	$\{A.N_a^i\}_{k_b}$	$\{A, B\}$	$\{A, B\}$	$\top$	Respected
X	A	$\{B.N_a^i\}_{k_a}.\{B.X\}_{k_a}$	$A.B.\{X\}_{k_b}$	$\{B\}$	$\ulcorner X \urcorner$	$\{A, B\}$	Respected
Y	B	$\{A.Y\}_{k_b}$	$\{Y.N_b^i.B\}_{k_a}$	$\{A, B\}$	$\ulcorner Y \urcorner$	$\{A, B\}$	Respected
N_b^i	B	$\{A.Y\}_{k_b}$	$\{Y.N_b^i.B\}_{k_a}$	$\{A, B\}$	$\{A, B\}$	$\{A, B\}$	Respected

Table 2: Compliance of NSL Protocol with the Theorem 6.5

the NSL protocol respects the correctness criterion stated in the theorem 6.5, then it is correct with respect to the secrecy property.

8. A VARIATION OF THE NEEDHAM-SCHROEDER PROTOCOL ANALYSIS WITH A WITNESS-FUNCTION

In this section, we analyze a variation of the Needham-Schroeder protocol with the witness-function. First,
let's recall it:

$$\begin{array}{llll} 1: & A & \longrightarrow & B: \{A.N_a\}_{k_b} \\ 2: & B & \longrightarrow & A: \{N_a.N_b.B\}_{k_a} \\ 3: & A & \longrightarrow & B: \{N_b\}_{k_b} \end{array}$$

The generalized roles of the protocol are $\mathcal{R}_{\mathcal{G}}^p = \{A_{\mathcal{G}}^l, A_{\mathcal{G}}^2, B_{\mathcal{G}}^l, B_{\mathcal{G}}^2\}$ where:

$$A_{\mathcal{G}}^l = \quad i.1 \quad A \longrightarrow I(B) : \{A.N_a^i\}_{k_b}$$

$$\begin{array}{lllll} A_{\mathcal{G}}^2 = & i.1 & A & \longrightarrow I(B) & : \{A.N_a^i\}_{k_b} \\ & i.2 & I(B) & \longrightarrow A & : \{N_a^i.X.B\}_{k_a} \\ & i.3 & A & \longrightarrow I(B) & : \{X\}_{k_b} \end{array}$$

$$\begin{array}{lllll} B_{\mathcal{G}}^l = & i.1 & I(A) & \longrightarrow B & : \{A.Y\}_{k_b} \\ & i.2 & B & \longrightarrow I(A) & : \{Y.N_b^i.B\}_{k_a} \end{array}$$

$$\begin{array}{lllll} B_{\mathcal{G}}^2 = & i.1 & I(A) & \longrightarrow B & : \{A.Y\}_{k_b} \\ & i.2 & B & \longrightarrow I(A) & : \{Y.N_b^i.B\}_{k_a} \\ & i.3 & I(A) & \longrightarrow B & : \{N_b^i\}_{k_b} \end{array}$$

Let's have a context of verification such that: $\ulcorner A \urcorner = \bot$; $\ulcorner B \urcorner = \bot$; $\ulcorner N_a^i \urcorner = \{A, B\}$ (secret between A and B); $\ulcorner N_b^i \urcorner = \{A, B\}$ (secret between A and B); $\ulcorner k_a^{-1} \urcorner = \{A\}$; $\ulcorner k_b^{-1} \urcorner = \{B\}$; $(\mathcal{L}, \sqsupseteq, \sqcup, \sqcap, \bot, \top) = (2^{\mathcal{I}}, \subseteq, \cap, \cup, \mathcal{I}, \emptyset)$; $\mathcal{I} = \{I(intruder), A, B, C, A_1, A_2, B_1, B_2, ...\}$;

The set of messages generated by the protocol is $\mathcal{M}_p^{\mathcal{G}} = \{\{A_1.N_{A_1}\}_{k_{B_1}}, \{N_{A_2}.X_1.B_2\}_{k_{A_2}}, \{X_2\}_{k_{B_3}}, \{A_3.Y_1\}_{k_{B_4}}, \{Y_2.N_{B_5}.B_5\}_{k_{A_4}}, \{N_{B_6}\}_{k_{B_6}}\}$;
The variables are denoted by X_1, X_2, Y_1 and Y_2;
The static names are denoted by $A_1, N_{A_1}, k_{B_1}, N_{A_2}, B_2, k_{A_2}, k_{B_3}, A_3, k_{B_4}, N_{B_5}, B_5, k_{A_4}, N_{B_6}$ and k_{B_6};

Let's select the Witness-Function as follows:
$p = NS$; $F = F_{MAX}^{EK}$; $\mathcal{W}_{p,F}(\alpha, m\sigma) = \underset{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = m\sigma}}{\sqcap} F(\alpha, \partial[\overline{\alpha}]m'\sigma')$;
Let's denote the lower bound of the Witness-Function by:

$$\mathcal{W}'_{p,F}(\alpha, r^+) = \underset{\substack{m' \in \mathcal{M}_p^{\mathcal{G}} \\ \exists \sigma' \in \Gamma. m'\sigma' = r^+\sigma'}}{\sqcap} F(\alpha, \partial[\overline{\alpha}]m'\sigma')$$

8.1 Results and interpretation

The results of the analysis of the variation of Needham-Schroeder protocol are summarized in Table 3.

α	Role	R^-	r^+	$\mathcal{W}'_{p,F}(\alpha, r^+)$	$\ulcorner \alpha \urcorner$	$F(\alpha, \partial[\overline{\alpha}]R^-)$	Theorem 6.5
N_a^i	A	$\emptyset$	$\{A.N_a^i\}_{k_b}$	$\{A, B\}$	$\{A, B\}$	$\top$	Respected
X	A	$\{N_a^i.X.B\}_{k_a}$	$\{X\}_{k_b}$	$\{B\}$	$\ulcorner X \urcorner$	$\{A, B\}$	Respected
Y	B	$\{A.Y\}_{k_b}$	$\{Y.N_b^i.B\}_{k_a}$	$\{A, B\}$	$\ulcorner Y \urcorner$	$\{A, B\}$	Respected
N_b^i	B	$\{A.Y\}_{k_b}$	$\{Y.N_b^i.B\}_{k_a}$	$\{A, B, A_3\}$	$\{A, B\}$	$\{A, B\}$	Not Respected

Table 3: Compliance of the Variation of Needham-Schroeder Protocol with the Theorem 6.5

We notice from the Table 3 that the variation of Needham-Schroeder protocol does not respect the correctness criterion set by the theorem 6.5 when analyzed with the witness-function $\mathcal{W}_{p_{NS}, F_{MAX}^{EK}}$. Therefore, we cannot deduce anything regarding its correctness with respect to the secrecy property. The non-growth of the protocol is localized in the sending step of the generalized role of B and it is due to a possible malicious neighbor (denoted by A_3 in our analysis) that could be inserted beside the nonce N_B^i. In the literature, we report a flaw that operates on the decay of the level of security of the nonce N_B^i in the generalized role of B. This flaw is described by the attack scenario in the Figure.1.

9. Conclusion And Future Work

In this paper, we gave relaxed conditions on interpretation functions to be reliable to run an analysis of a cryptographic protocol on valid traces for the property of secrecy. Afterward, we gave a whole class of reliable functions based on selections inside the external key. Then we introduced the witness-functions that offer two bounds which are independent of substitutions and therefore enable an analysis on the generalized roles of a protocol in a role-based specification. We experimented our approach on real protocols and we showed that a witness-function can even help to locate flaws. It was successful to prove the correctness of others too. In a future work, we intend to define more witness-functions based on the selection inside other keys (other than the most external key) like the most internal key or all encryption keys together, so that we could efficiently deal with algebraic properties in a non-empty equational theory [19–21] such the Diffie-Hellman property. We intend also to take advantage of the bounds of witness-functions to consider exchanged messages in a protocol as encryption keys.

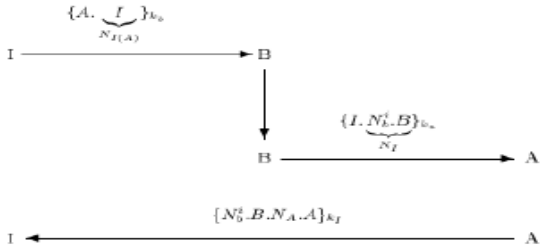

Figure 1: Attack Scenario on the Variation of the Needham-Schroeder Protocol

REFERENCES

[1] S. Schneider, "Verifying authentication protocols in csp," IEEE Trans. Software Eng., vol. 24, no. 9, pp. 741–758, 1998.

[2] S. Schneider, "Security properties and csp," in IEEE Symposium on Security and Privacy, pp. 174–187, 1996.

[3] S. A. Schneider and R. Delicata, "Verifying security protocols: An application of csp," in 25 Years Communicating Sequential Processes, pp. 243–263, 2004.

[4] J. Heather and S. Schneider, "A decision procedure for the existence of a rank function," J. Comput. Secur., vol. 13, pp. 317–344, Mar. 2005.

[5] M. Abadi, "Secrecy by typing in security protocols," Journal of the ACM, vol. 46, pp. 611–638, 1998.

[6] M. Abadi and A. D. Gordon, "Reasoning about cryptographic protocols in the spi calculus," in CONCUR, pp. 59–73, 1997.

[7] M. Abadi and A. D. Gordon, "A calculus for cryptographic protocols: The spi calculus," in ACM Conference on Computer and Communications Security, pp. 36–47, 1997.

[8] H. Houmani and M. Mejri, "Practical and universal interpretation functions for secrecy," in SECRYPT, pp. 157–164, 2007.

[9] H. Houmani and M. Mejri, "Ensuring the correctness of cryptographic protocols with respect to secrecy," in SECRYPT, pp. 184–189, 2008.

[10] H. Houmani and M. Mejri, "Formal analysis of set and nsl protocols using the interpretation functions-based method," Journal Comp. Netw. and Communic., vol. 2012, 2012.

[11] H. Houmani, M. Mejri, and H. Fujita, "Secrecy of cryptographic protocols under equational theory," Knowl.-Based Syst., vol. 22, no. 3, pp. 160–173, 2009.

[12] D. Dolev and A. C.-C. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–207, 1983.

[13] J. Fattahi, M. Mejri, and H. Houmani, "Context of verification and role-based specification http://web_security.fsg.ulaval.ca/lab/sites/default/files/WF/Ind/Context.pdf," no. 4, pp. 1–4, 2014.

[14] M. Debbabi, Y. Legaré, and M. Mejri, "An environment for the specification and analysis of cryptoprotocols," in ACSAC, pp. 321–332, 1998.

[15] M. Debbabi, M. Mejri, N. Tawbi, and I. Yahmadi, "Formal automatic verification of authentication crytographic protocols," in ICFEM, pp. 50–59, 1997.

[16] M. Debbabi, M. Mejri, N. Tawbi, and I. Yahmadi, "From protocol specifications to flaws and attack scenarios: An automatic and formal algorithm," in WETICE, pp. 256–262, 1997.

[17] J. Fattahi, M. Mejri, and H. Houmani, "The witness-functions: Proofs and intermediate results. http://web_security.fsg.ulaval.ca/lab/sites/default/files/WF/Ind/WitFunProofs.pdf,"no. 26, pp. 1–26, 2014.

[18] B. Blanchet, "Automatic verification of correspondences for security protocols," Journal of Computer Security, vol. 17, no. 4, pp. 363–434, 2009.

[19] H. Comon-Lundh, V. Cortier, and E. Zalinescu, "Deciding security properties for cryptographic protocols. application to key cycles," ACM Trans. Comput. Log., vol. 11, no. 2, 2010.

[20] V. Cortier and S. Delaune, "Decidability and combination results for two notions of knowledge in security protocols," J. Autom. Reasoning, vol. 48, no. 4, pp. 441–487, 2012.

[21] V. Cortier, S. Kremer, and B. Warinschi, "A survey of symbolic methods in computational analysis of cryptographic systems," J. Autom. Reasoning, vol. 46, no. 3-4, pp. 225–259, 2011.

[22] F. Baader and T. Nipkow, Term rewriting and all that. Cambridge University Press, 1998.

[23] N. Dershowitz and D. A. Plaisted, "Rewriting," in Handbook of Automated Reasoning, pp. 535–610, 2001.

[24] H. Comon-Lundh, C. Kirchner, and H. Kirchner, eds., Rewriting, Computation and Proof, Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of His 60th Birthday, vol. 4600 of Lecture Notes in Computer Science, Springer, 2007.