Vérification de protocoles de sécurité dans un modèle de l'intrus étendu

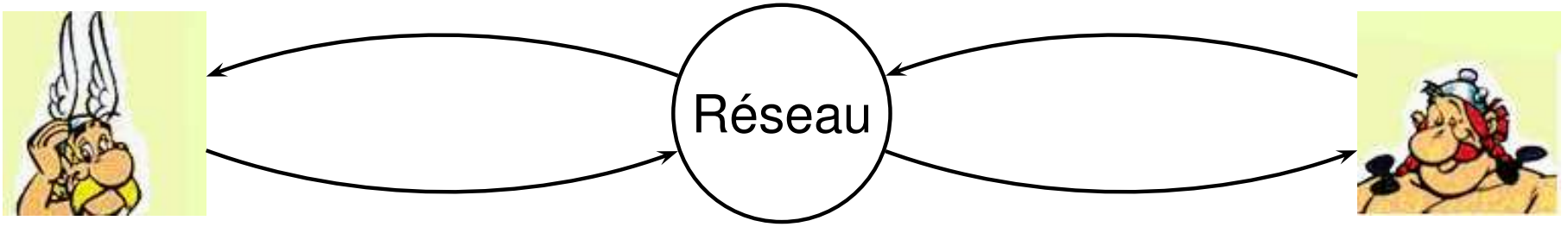
Stéphanie Delaune

delaune@lsv.ens-cachan.fr

Laboratoire de Spécification et de Vérification
CNRS UMR 8643
École Normale Supérieure de Cachan
CACHAN - France

Laboratoire Spécification et Vérification

Protocoles cryptographiques



Protocole

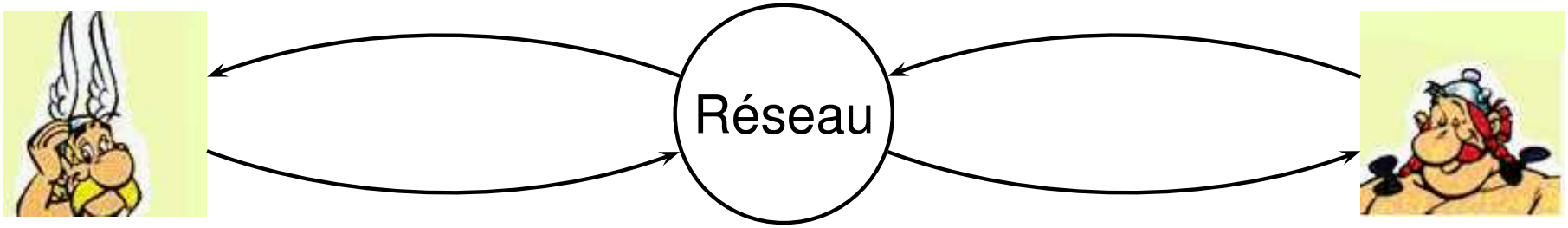
↪ règles d'échange de messages

But

↪ sécuriser les communications: *confidentialité, authenticité, ...*

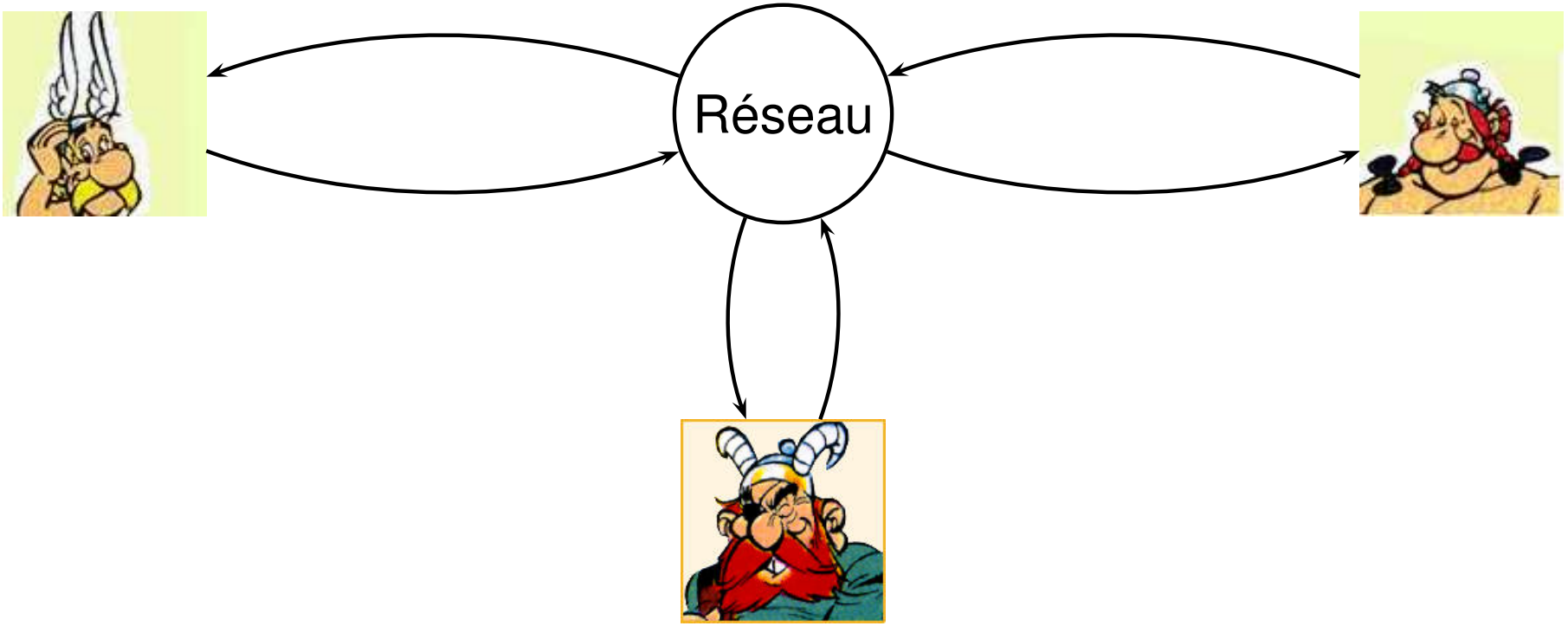
Protocoles cryptographiques

L'intrus ....



Protocoles cryptographiques

L'intrus ....



Protocoles cryptographiques

L'intrus ....

Protocoles cryptographiques

Messages $\rightsquigarrow$ termes

- $\hookrightarrow$ paire $\langle m_1, m_2 \rangle$
- $\hookrightarrow$ chiffrement $\{m\}_k$ (symétrique /asymétrique)
- $\hookrightarrow$ clef inverse k^{-1}
- $\hookrightarrow$ $pub(a)$, $h(m)$ ...

Intrus $\rightsquigarrow$ système de règles d'inférence

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao

Soit u, v des termes et T un ensemble fini de termes:

Axiome (A) $\dfrac{u \in T}{T \vdash u}$

Paire (P) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$

Projection (UL) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$

Projection (UR) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$

Chiffrement (E) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$

Déchiffrement (D) $\dfrac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao

Soit u, v des termes et T un ensemble fini de termes:

Axiome (A) $\dfrac{u \in T}{T \vdash u}$

Paire (P) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$

Projection (UL) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$

Projection (UR) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$

Chiffrement (E) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$

Déchiffrement (D) $\dfrac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao

Soit u, v des termes et T un ensemble fini de termes:

Axiome (A) $\dfrac{u \in T}{T \vdash u}$

Paire (P) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$

Projection (UL) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$

Projection (UR) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$

Chiffrement (E) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$

Déchiffrement (D) $\dfrac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$

Le modèle de Dolev-Yao

Soit u, v des termes et T un ensemble fini de termes:

Axiome (A) $\dfrac{u \in T}{T \vdash u}$

Paire (P) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$

Projection (UL) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$

Projection (UR) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$

Chiffrement (E) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$

Déchiffrement (D) $\dfrac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$

$\hookrightarrow$ **Hypothèse du chiffrement parfait**

aucune information sur u à partir de $\{u\}_v$ sans connaître v^{-1}

Le problème de déduction de l'intrus: $T \stackrel{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*
- Un message: s,
  $\hookrightarrow$ *le message pour lequel on veut vérifier le secret*

QUESTION:

- L'intrus peut-il déduire le secret s à partir de T ?

Laboratoire Spécification et Vérification

Rappel des résultats

Le problème de déduction de l'intrus dans le modèle de Dolev-Yao

Théorème: [Comon & Shmatikov, 2003]

La théorie de Dolev-Yao est *locale* [Mc Allester, 1993]:
S'il existe une preuve de $T \vdash s$, alors il existe une preuve qui n'utilise que des sous-termes des termes de $T \cup \{s\}$.

Conséquence:

Le problème de déduction de l'intrus, $T \overset{?}{\vdash} s$, est PTIME complet.

Faiblesses de l'existant

sur le plan de la modélisation de l'intrus

- le chiffrement n'est pas parfait

  ↪ *les algorithmes de chiffrement possèdent des propriétés algébriques*

- les « attaques par prédictions » [DEA]

  ↪ *l'intrus peut en construisant et comparant des messages obtenir de l'information sur un message chiffré*

Faiblesses de l'existant

sur le plan de la modélisation de l'intrus

- le chiffrement n'est pas parfait
  ↪ *les algorithmes de chiffrement possèdent des propriétés algébriques*
- les « attaques par prédictions » [DEA]
  ↪ *l'intrus peut en construisant et comparant des messages obtenir de l'information sur un message chiffré*

sur le plan de la vérification pratique

- une unique propriété
  ↪ *le secret*
- un unique modèle d'intrus [DEA]
  ↪ *le modèle de Dolev-Yao*

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

- deviner la valeur choisie par A: v_i

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

- deviner la valeur choisie par A: v_i
- construire le message $\{v_i\}_{pub(S)}$

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

- deviner la valeur choisie par A: v_i
- construire le message $\{v_i\}_{pub(S)}$
- le comparer avec le message intercepté: $\{vote\}_{pub(S)}$.

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

- deviner la valeur choisie par A: v_i
- construire le message $\{v_i\}_{pub(S)}$
- le comparer avec le message intercepté: $\{vote\}_{pub(S)}$.

Conséquence:

l'intrus connaît le vote de A.

Exemple 2 - challenge

Considérons l'échange suivant: [Gong 93]

$$\begin{aligned} A &\rightarrow B : \quad \{n\}_k \\ B &\rightarrow A : \quad \{n+1\}_k \end{aligned}$$

où $k \in \{k_1, ..., k_n\}$ est une clef symétrique et n un nonce.

Exemple 2 - challenge

Considérons l'échange suivant: [Gong 93]

$$\begin{aligned} A &\rightarrow B : \quad \{n\}_k \\ B &\rightarrow A : \quad \{n+1\}_k \end{aligned}$$

où $k \in \{k_1, ..., k_n\}$ est une clef symétrique et n un nonce.

Description de l'attaque:

- deviner la valeur de k : k_i
- déchiffrer les deux messages interceptés, $\{n\}_k$ et $\{n+1\}_k$ avec la clef choisie k_i
- comparer les deux valeurs obtenues.

Exemple 2 - challenge

Considérons l'échange suivant: [Gong 93]

$$\begin{aligned} A &\rightarrow B : \quad \{n\}_k \\ B &\rightarrow A : \quad \{n+1\}_k \end{aligned}$$

où $k \in \{k_1, ..., k_n\}$ est une clef symétrique et n un nonce.

Description de l'attaque:

- deviner la valeur de k : k_i
- déchiffrer les deux messages interceptés, $\{n\}_k$ et $\{n+1\}_k$ avec la clef choisie k_i
- comparer les deux valeurs obtenues.

Conséquence:

l'intrus connaît la clef k, et le nonce n.

Contributions du stage

I) Modélisation des attaques par prédictions

- Présentation du «nouveau» problème de déduction de l'intrus
- Présentation du modèle de Dolev-Yao étendu
- Résultats

II) Vérification pratique des protocoles

- Securify: un outil de vérification du secret
- Prototype: une procédure de recherche d'attaques

Le problème de déduction de l'intrus: $T/T' \stackrel{?}{\vdash} s$

Laboratoire Spécification et Vérification

Le problème de déduction de l'intrus: $T/T' \overset{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages «fortement connus»: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*

Le problème de déduction de l'intrus: $T/T' \stackrel{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages «fortement connus»: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*
- Un ensemble fini de données atomiques, «faiblement connues»: T',
  $\hookrightarrow$ *typiquement, les données qui prennent leur valeur dans un domaine fini connu de l'intrus*

Le problème de déduction de l'intrus: $T/T' \stackrel{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages «fortement connus»: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*
- Un ensemble fini de données atomiques, «faiblement connues»: T',
  $\hookrightarrow$ *typiquement, les données qui prennent leur valeur dans un domaine fini connu de l'intrus*
- Un message: s,
  $\hookrightarrow$ *le message pour lequel on veut vérifier le secret*

Le problème de déduction de l'intrus: $T/T' \stackrel{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages «fortement connus»: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*
- Un ensemble fini de données atomiques, «faiblement connues»: T',
  $\hookrightarrow$ *typiquement, les données qui prennent leur valeur dans un domaine fini connu de l'intrus*
- Un message: s,
  $\hookrightarrow$ *le message pour lequel on veut vérifier le secret*

QUESTION:

- L'intrus peut-il déduire le secret s à partir de T et T' ?

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$

  $\hookrightarrow$ *L'intrus peut déduire «fortement»* u *à partir de* T *et* T'

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$

  $\hookrightarrow$ *L'intrus peut déduire «fortement»* u *à partir de* T *et* T'

- **Déduction faible:** $T/T' \vdash' u$

  $\hookrightarrow$ *L'intrus peut déduire «faiblement»* u *à partir de* T *et* T'

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$

  $\hookrightarrow$ *L'intrus peut déduire «fortement»* u *à partir de* T *et* T'

- **Déduction faible:** $T/T' \vdash' u$

  $\hookrightarrow$ *L'intrus peut déduire «faiblement»* u *à partir de* T *et* T'

Exemple - *la règle Axiome*

$$\frac{u \in T}{T \vdash u}$$

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$
  ↪ *L'intrus peut déduire «fortement» u à partir de T et T'*
- **Déduction faible:** $T/T' \vdash' u$
  ↪ *L'intrus peut déduire «faiblement» u à partir de T et T'*

Exemple - *la règle Axiome*

$$\frac{u \in T}{T \vdash u}$$

$$\text{(A)}\quad \frac{u \in T}{T/\emptyset \vdash u} \qquad \frac{u \text{ terme atomique}}{T/u \vdash' u}\quad \text{(A')}$$

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$
  ↪ *L'intrus peut déduire «fortement»* u *à partir de* T *et* T'
- **Déduction faible:** $T/T' \vdash' u$
  ↪ *L'intrus peut déduire «faiblement»* u *à partir de* T *et* T'

Exemple - *la règle Paire*

$$\frac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$$

$$\swarrow \qquad \searrow$$

$$\text{(P)} \quad \frac{T/T'_1 \vdash u \quad T/T'_2 \vdash v}{T/T'_1 \cup T'_2 \vdash \langle u, v \rangle} \qquad \frac{T/T'_1 \vdash' u \quad T/T'_2 \vdash' v}{T/T'_1 \cup T'_2 \vdash' \langle u, v \rangle} \quad \text{(P}')$$

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$
  $\hookrightarrow$ *L'intrus peut déduire «fortement»* u *à partir de* T *et* T'
- **Déduction faible:** $T/T' \vdash' u$
  $\hookrightarrow$ *L'intrus peut déduire «faiblement»* u *à partir de* T *et* T'

Exemple - *La règle Affaiblissement*

$$(\mathsf{W}) \quad \frac{u \in T}{T/\emptyset \vdash' u}$$

Déduction forte

(A) $$\frac{u \in T}{T/\emptyset \vdash u}$$

(P) $$\frac{T/T'_1 \vdash u \quad T/T'_2 \vdash v}{T/T'_1 \cup T'_2 \vdash \langle u, v \rangle}$$

(UL) $$\frac{T/T' \vdash \langle u, v \rangle}{T/T' \vdash u}$$

(UR) $$\frac{T/T' \vdash \langle u, v \rangle}{T/T' \vdash v}$$

(E) $$\frac{T/T'_1 \vdash u \quad T/T'_2 \vdash v}{T/T'_1 \cup T'_2 \vdash \{u\}_v}$$

(D) $$\frac{T/T'_1 \vdash \{u\}_v \quad T/T'_2 \vdash v^{-1}}{T/T'_1 \cup T'_2 \vdash u}$$

Déduction faible

$$(\mathsf{A}') \quad \frac{u \text{ terme atomique}}{T/u \vdash' u} \qquad (\mathsf{P}') \quad \frac{T/T_1' \vdash' u \quad T/T_2' \vdash' v}{T/T_1' \cup T_2' \vdash' \langle u, v \rangle}$$

$$(\mathsf{UL}') \quad \frac{T/T' \vdash' \langle u, v \rangle}{T/T' \vdash' u} \qquad (\mathsf{UR}') \quad \frac{T/T' \vdash' \langle u, v \rangle}{T/T' \vdash' v}$$

$$(\mathsf{E}') \quad \frac{T/T_1' \vdash' u \quad T/T_2' \vdash' v}{T/T_1' \cup T_2' \vdash' \{u\}_v} \qquad (\mathsf{D}') \quad \frac{T/T_1' \vdash' \{u\}_v \quad T/T_2' \vdash' v^{-1}}{T/T_1' \cup T_2' \vdash' u}$$

Laboratoire Spécification et Vérification

La règle Comparaison ($1^{ère}$ version)

$$\dfrac{P_1\left\{\dfrac{\dfrac{..}{\vdash' x_1}\ldots\dfrac{..}{\vdash' x_n}}{T/T_1' \vdash' v}\ (R1)\right. \qquad P_2\left\{\dfrac{\dfrac{..}{\vdash' y_1}\ldots\dfrac{..}{\vdash' y_n}}{T/T_2' \vdash' v}\ (R2)\right.}{T/T_1' \cup T_2' \vdash w}\ (Comp)$$

où:

(i). $w \in T_1' \cup T_2'$

(ii). R1 $\neq$ R2 ou $\{x_1, .., x_n\} \neq \{y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

Laboratoire Spécification et Vérification

La règle Comparaison ($1^{ère}$ version)

$$\dfrac{P_1\left\{\dfrac{\dfrac{..}{\vdash' x_1}\ldots\dfrac{..}{\vdash' x_n}}{T/T_1' \vdash' v}\ (R1)\right. \qquad P_2\left\{\dfrac{\dfrac{..}{\vdash' y_1}\ldots\dfrac{..}{\vdash' y_n}}{T/T_2' \vdash' v}\ (R2)\right.}{T/T_1' \cup T_2' \vdash w}\ (Comp)$$

où:

(i). $w \in T_1' \cup T_2'$

(ii). R1 $\neq$ R2 ou $\{x_1, .., x_n\} \neq \{y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

La règle Comparaison ($1^{ère}$ version)

$$\dfrac{P_1\left\{\dfrac{\dfrac{..}{\vdash' x_1}\cdots\dfrac{..}{\vdash' x_n}}{T/T_1' \vdash' v}\ (\text{R1})\right. \qquad P_2\left\{\dfrac{\dfrac{..}{\vdash' y_1}\cdots\dfrac{..}{\vdash' y_n}}{T/T_2' \vdash' v}\ (\text{R2})\right.}{T/T_1' \cup T_2' \vdash w}\ (\text{Comp})$$

où:

(i). $w \in T_1' \cup T_2'$

(ii). R1 $\neq$ R2 ou $\{x_1, .., x_n\} \neq \{y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

Laboratoire Spécification et Vérification

La règle Comparaison ($1^{ère}$ version)

$$\dfrac{P_1\left\{\dfrac{\dfrac{..}{\vdash' x_1}\ldots\dfrac{..}{\vdash' x_n}}{T/T_1' \vdash' v}\ (R1)\right. \qquad P_2\left\{\dfrac{\dfrac{..}{\vdash' y_1}\ldots\dfrac{..}{\vdash' y_n}}{T/T_2' \vdash' v}\ (R2)\right.}{T/T_1' \cup T_2' \vdash w}\ (Comp)$$

où:

(i). $w \in T_1' \cup T_2'$

(ii). R1 $\neq$ R2 ou $\{x_1, .., x_n\} \neq \{y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

La règle Comparaison

$$\dfrac{P_1\left\{\dfrac{\dfrac{..}{\vdash' x_1}\cdots\dfrac{..}{\vdash' x_n}}{T/T_1' \vdash' u}\ (R1)\right. \qquad P_2\left\{\dfrac{\dfrac{..}{\vdash' y_1}\cdots\dfrac{..}{\vdash' y_n}}{T/T_2' \vdash' v}\ (R2)\right.}{T/T_1' \cup T_2' \vdash w}\ (Comp)$$

où:

(i). $w \in T_1' \cup T_2'$

(ii). R1 $\neq$ R2 ou $\{v, x_1, .., x_n\} \neq \{v, y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

(iv). $R(u, v)$ où $R = Id \cup \{(k, k^{-1}) |$ k est une clef$\}$

Exemple 1 - protocole naïf de vote

$$A \rightarrow S : \{v\}_{pub(S)}$$

$$T = \{\{v\}_{pub(S)}, pub(S)\}$$
$$T' = \{v\}$$

Exemple 1 - protocole naïf de vote

$$A \to S : \{v\}_{pub(S)}$$

$$T = \{\{v\}_{pub(S)}, pub(S)\}$$
$$T' = \{v\}$$

Nous avons la dérivation suivante:

$$\dfrac{\dfrac{\dfrac{}{T/\{v\} \vdash' v}\,\mathsf{A}' \quad \dfrac{pub(S) \in T}{T/\emptyset \vdash' pub(S)}\,\mathsf{W}}{T/\{v\} \vdash' \{v\}_{pub(S)}}\,\mathsf{E}' \quad \dfrac{\{v\}_{pub(S)} \in T}{T/\emptyset \vdash' \{v\}_{pub(S)}}\,\mathsf{W}}{T/\{v\} \vdash v}\,\mathsf{C}$$

Exemple 2 - challenge

$$A \rightarrow B : \{n\}_k \qquad T = \{\{n\}_k, \{n+1\}_k\}$$
$$B \rightarrow A : \{n+1\}_k \qquad T' = \{k\}$$

Laboratoire Spécification et Vérification

Exemple 2 - challenge

$$A \rightarrow B : \{n\}_k \qquad T = \{\{n\}_k, \{n+1\}_k\}$$
$$B \rightarrow A : \{n+1\}_k \qquad T' = \{k\}$$

Nous avons la dérivation suivante:

$$\dfrac{\dfrac{\dfrac{\{n\}_k \in T}{T/\emptyset \vdash' \{n\}_k} \quad \dfrac{}{T/\{k\} \vdash' k}}{T/\{k\} \vdash' n}}{T/\{k\} \vdash' n+1} \qquad \dfrac{\dfrac{\dfrac{\{n+1\}_k \in T}{T/\emptyset \vdash' \{n+1\}_k} \quad \dfrac{}{T/\{k\} \vdash' k}}{T/\{k\} \vdash' n+1}}{T/\{k\} \vdash k}\ C$$

Résultats

Le problème de déduction de l'intrus dans le modèle étendu

Théorème 1:

La théorie de Dolev-Yao étendu est *locale* :
S'il existe une preuve de $T/T' \vdash s$, alors il existe une preuve qui n'utilise que des sous-termes des termes de $T \cup T' \cup \{s\}$.

Théorème 2:

Le problème de déduction de l'intrus, $T/T' \stackrel{?}{\vdash} s$, est PTIME.

Plan

I) Modélisation des attaques par prédictions

- Présentation du «nouveau» problème de déduction de l'intrus
- Présentation du modèle de Dolev-Yao étendu
- Résultats

II) Vérification pratique des protocoles

- Securify: un outil de vérification du secret

  ↪ Présentation de Securify

  ↪ Amélioration de Securify
- Prototype: une procédure de recherche d'attaques

Présentation de Securify

Outil disponible en ligne, à l'adresse: `http://www-eva.imag.fr/outils1.html`

Entrée:

- un protocole
- une propriété de secret

Sortie:
La réponse à la question: «le secret est-il vérifié?»

↪ si oui, l'arbre de preuve

↪ si non, l'arbre d'échec de la preuve

↪ pas de réponse, l'outil ne termine pas

Laboratoire Spécification et Vérification

Présentation de Securify

Outil disponible en ligne, à l'adresse: `http://www-eva.imag.fr/outils1.html`

Entrée:

- un protocole
- une propriété de secret

Sortie:
La réponse à la question: «le secret est-il vérifié?»

↪ si oui, l'arbre de preuve

↪ si non, l'arbre d'échec de la preuve

↪ pas de réponse, l'outil ne termine pas

Points faibles:

- une unique propriété: *le secret long terme*
- un unique modèle d'intrus: *le modèle de Dolev-Yao*

Laboratoire Spécification et Vérification

Amélioration de Securify

Résultats:

Protocoles		Preuve dans	
		Securify	Securify amélioré
Otway-Rees		Oui	Oui
Needham-Schroeder-Lowe	*secret de Na, Nb*	Oui	Oui
	secret de Na	Non?	Oui
	secret de Nb	Non?	Oui
Needham-Schroeder	*secret de Na, Nb*	Non	Non
	secret de Na	Non?	Oui
	secret de Nb	Non	Non
Yahalom		Non?	Oui
RPC Secure		Non?	Oui

Laboratoire Spécification et Vérification

Plan

I) Modélisation des attaques par prédictions

- Problème de déduction de l'intrus dans le modèle de Dolev-Yao
- Problème de déduction de l'intrus dans le modèle étendu

II) **Vérification pratique des protocoles**

- Securify: un outil de vérification du secret
- Prototype: une procédure de recherche d'attaques
  - ↪ Présentation du prototype
  - ↪ Architecture du prototype
  - ↪ Résultats

Laboratoire Spécification et Vérification

Présentation du prototype

But:

Expérimenter le nouveau modèle d'intrus en implémentant un outil de recherche d'attaques

Entrée:

- un protocole
- les instances des sessions considérées
- une propriété de secret
- un module d'intrus

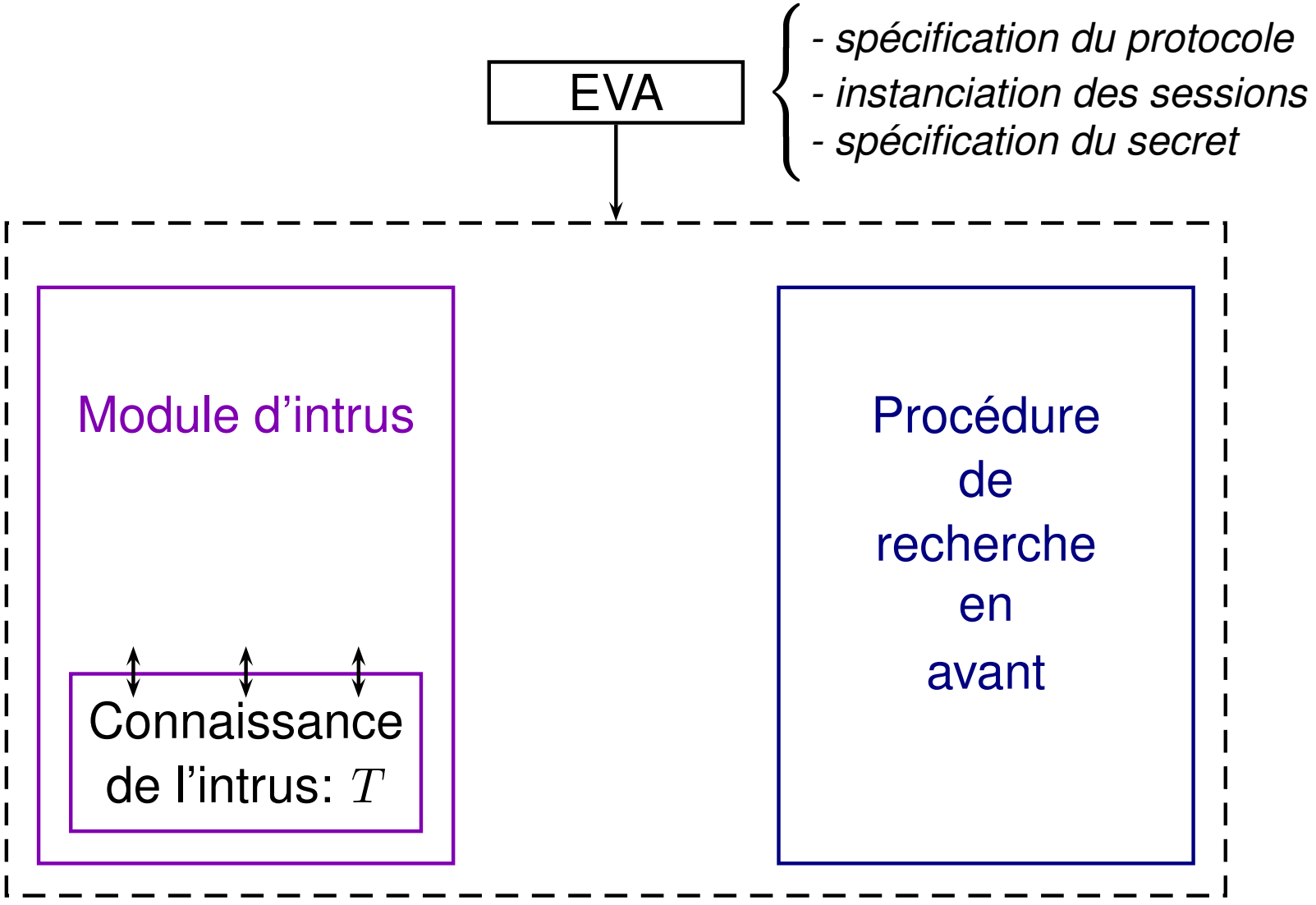
Sortie:

La réponse à la question: «le secret est-il déductible par l'intrus»

$\hookrightarrow$ si oui, description de l'attaque

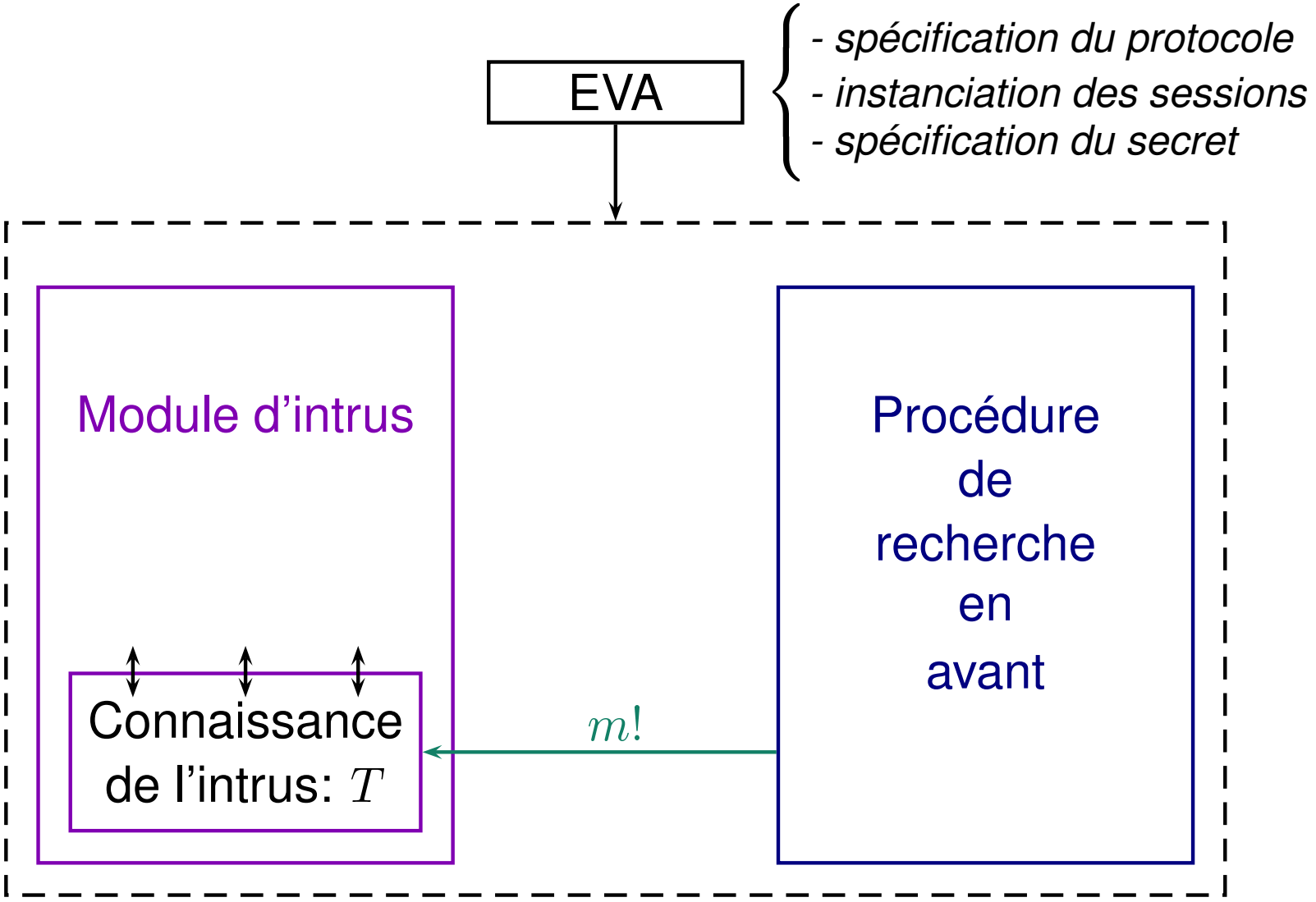
Laboratoire Spécification et Vérification

Architecture du prototype

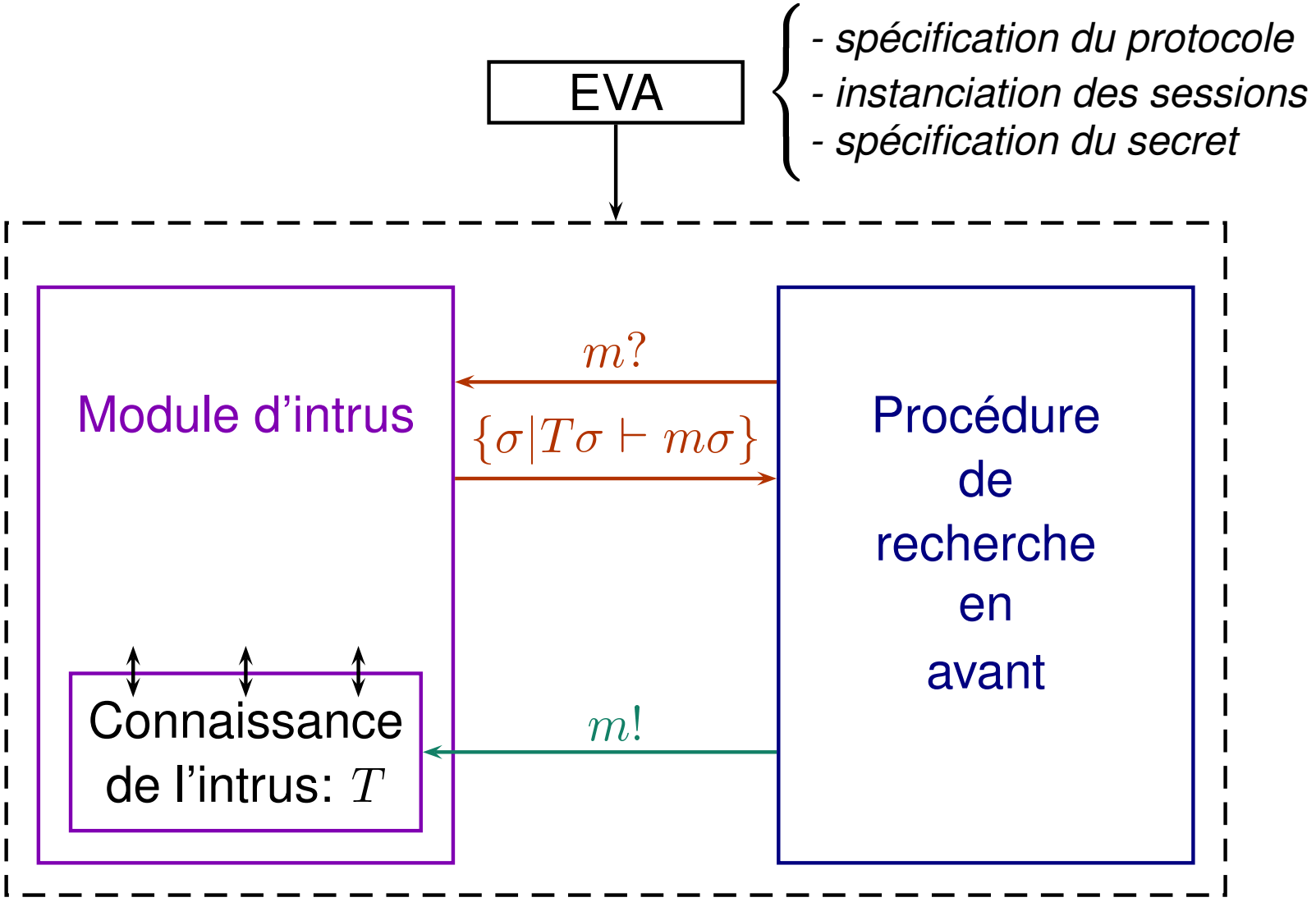


Laboratoire Spécification et Vérification

Architecture du prototype



Architecture du prototype



Exemple - le protocole de Vote

```
Vote

constant keypair PK, SK (principal):number
parameter S, A : principal
parameter fresh N: weak
S knows S, PK, SK(S)
A knows A, S, N, PK

{ 1. A -> S : {N}_PK(S) }

value a, s: principal
value na:number
s1. session (A=a; S=s; N=na)

claim secret(na)
```

Laboratoire Spécification et Vérification

Résultats

↪ exécution normale d'une session du protocole

Protocole	Modèle d'intrus			
	Dolev-Yao standard		Dolev-Yao étendu	
	attaque	temps (ms)	attaque	temps (ms)
Vote	Non	20	Oui	20
Challenge	Non	20	Oui	20
Andrew Secure RPC	Non	110	Oui	60
Clefs asymétriques	Non	20	Oui	30
Echange Gong	Non	60	Non	310
Echange Gong modifié	Non	30	Oui	70
Bellovin et Merritt	Non	50	Non	220
Bellovin et Merritt modifié	Non	50	Oui	110

Conclusion

- présentation d'un nouveau modèle d'intrus
  - ↪ pour prendre en compte les «attaques par prédictions»
- $T/T' \overset{?}{\vdash} s$ est PTIME
- amélioration de l'outil Securify
- implémentation d'une procédure de recherche d'attaques paramétrée par une théorie de l'intrus:
  - ↪ théorie de Dolev-Yao
  - ↪ théorie de Dolev-Yao étendue

Perspectives

- résultat de décidabilité et de complexité de préservation du secret pour un nombre borné de sessions

  $\hookrightarrow$ généraliser les résultats obtenus pour $T/T' \stackrel{?}{\vdash} s$, aux termes avec variables

- considérer d'autres modèles d'intrus

  $\hookrightarrow$ pour prendre en compte les propriétés algébriques des primitives cryptographiques

- développer une procédure de recherche de preuves paramétrée par la théorie de l'intrus

Laboratoire Spécification et Vérification