TD 3: Deduction system for the symbolic setting

Margot Catinaud margot.catinaud@lmf.cnrs.fr
Théo Vignon theo.vignon@lmf.cnrs.fr

November 29, 2024

Exercise 1: Unification

For each pair of terms, check if those are unifiable or not (find a most general unifier if possible). Here, b and a are function symbols.

1. $\langle x\,,\,\mathsf{b}\rangle$ and $\langle \mathsf{a}\,,\,x\rangle$
2. $\langle \mathsf{b}\,,\,x\rangle$ and $\langle \mathsf{a}\,,\,y\rangle$
3. $\{x\}_{\mathsf{a}}$ and $\{\mathsf{b}\}_x$
4. $\langle x\,,\,y\rangle$ and $\langle\langle y\,,\,y\rangle\,,\,x\rangle$
5. $\langle \mathsf{a}\,,\,y\rangle$ and $\langle\langle y\,,\,y\rangle\,,\,\mathsf{a}\rangle$
6. z and $\langle x\,,\,y\rangle$

Exercise 2: A first deduction system

Consider the following deduction system:

$$\frac{x \quad y}{\langle x\,,\,y\rangle} \qquad \frac{\langle x\,,\,y\rangle}{x} \qquad \frac{\langle x\,,\,y\rangle}{y}$$

$$\frac{x \quad y}{\{x\}_y} \qquad\qquad \frac{\{x\}_y \quad y}{x}$$

1. Give the signature used by this deduction system? Is the encryption symmetric or asymmetric?

Consider the set of terms:

$$\mathsf{T} = \left\{\{\mathsf{s}\}_{\langle \mathsf{k}_1\,,\,\mathsf{k}_2\rangle},\ \{\mathsf{k}_1\}_{\mathsf{k}_3},\ \mathsf{k}_3,\ \mathsf{k}_2\right\}$$

2. Enumerate all the subterms of T
3. the term s is deducible from T. Give a derivation witnessing this fact.
4. Among the subterms of T, give those that are deducible.
5. Give a term u that is not a subterm of T and such that $\mathsf{T} \vdash \mathsf{u}$

Exercise 3: Various Primitives

For each primitive, give a set of deduction rules that represent the primitive. (You can assume that you have the pair and booleans in your signature if you wish)

1. *symmetric encryption:* the corresponding signature is $\{\mathsf{senc}/2,\ \mathsf{sdec}/2\}$.
2. *asymmetric encryption:* the corresponding signature is $\{\mathsf{aenc}/2,\ \mathsf{adec}/2,\ \mathsf{pk}/1\}$.
3. *signature:* the corresponding signature is $\{\mathsf{sign}/2, \mathsf{verify}/3, \mathsf{signkey}/1\}$.
4. *authenticated encryption with associated data:* the corresponding signature is $\{\ \mathsf{enc}_{\mathsf{aead}}/3, \mathsf{enc}_{\mathsf{aead}}/3\}$.

Exercise 4: Intruder deduction problem and locality

Recall the definition of locality for a deduction system and the intruder deduction problem:

Definition: Locality

A deduction system $\mathcal{D}$ is local if for all T finite set of terms and term s such that $\mathsf{T} \vdash \mathsf{s}$, there is a proof tree Π of that fact such that $\mathsf{Terms}(\Pi) \subseteq \mathsf{st}(\mathsf{T} \cup \{\mathsf{s}\})$.
Where $\mathsf{Terms}(\Pi)$ is the set of terms that appear in a given proof tree Π and $\mathsf{st}(\mathsf{E})$ is the set of sub-terms of terms in E.

Definition: Intruder deduction problem

Let $\mathcal{I}$ be an inference system. The intruder deduction problem is:

Input: a finite set of terms T and a term s

Output: whether $\mathsf{T} \vdash_{\mathcal{I}} \mathsf{s}$

1. Show that the intruder deduction problem is decidable for a local deduction system
   Hint: You can find a PTIME algorithm that decides this problem
2. Can you find an inference system for which the intruder deduction problem is undecidable?

Exercise 5: Dolev-Yao inference system

Consider the following deduction system:

$$\frac{x \quad y}{\langle x\,,\, y\rangle} \qquad \frac{\langle x\,,\, y\rangle}{x} \qquad \frac{\langle x\,,\, y\rangle}{y}$$

$$\frac{x \quad y}{\mathsf{senc}(x,y)} \qquad \frac{\mathsf{senc}(x,y) \quad y}{x}$$

$$\frac{x \quad y}{\mathsf{aenc}(x,y)} \qquad \frac{\mathsf{aenc}(x,\mathsf{pk}(y)) \quad y}{x}$$

1. Show that it is local
   Hint: for that, a valid proof tree to consider is any minimal (in the number of terms (with multiplicity)) proof tree.
2. Conclude that the intruder deduction system is decidable on this inference system

We are now interested in a new procedure for deciding if a term s is deducible from a set of term T in the inference system described above, we propose the following algorithm:

Exercise 5: Dolev-Yao inference system

Algorithm:

- Apply the decryption and projection rules as much as possible. This leads to a (finite) set of terms called $\texttt{analz}(\mathsf{T})$
- Check whether s can be obtained by applying the encryption and the pairing rules. The (infinite) set of terms obtained by applying the composition rules is denoted $\texttt{synth}(\texttt{analz}(\mathsf{T}))$.
- Return $\mathsf{s} \in \texttt{synth}(\texttt{analz}(\mathsf{T}))$

3. Show that this algorithm terminates
4. Show that this algorithm is sound, i.e. if the algorithm returns yes then $\mathsf{T} \vdash \mathsf{s}$
5. The algorithm is not complete, i.e. there exists T and s such that $\mathsf{T} \vdash \mathsf{s}$, and for which the algorithm returns no. Find an example illustrating this fact.
6. Give a hypothesis on T that allows one to restore completeness.
7. Show that the algorithm is complete with this added hypothesis.

Exercise 6: Blind signature and intruder deduction problem

In this exercise, we consider *blind signatures* represented by the following inference system:

Definition: Blind signatures inference system $\mathcal{I}_{\mathsf{blind}}$

$$\frac{x \quad y}{\langle x\,,\, y\rangle} \qquad \frac{\langle x\,,\, y\rangle}{x} \qquad \frac{\langle x\,,\, y\rangle}{y}$$

$$\frac{x \quad y}{\mathsf{blind}(x,y)} \qquad \frac{x \quad y}{\mathsf{sign}(x,y)}$$

$$\frac{\mathsf{sign}(\mathsf{blind}(x,y),z) \quad y}{\mathsf{sign}(x,z)} \qquad \frac{\mathsf{blind}(x,y) \quad y}{x}$$

1. Find a set of messages T and a name n such that $\mathsf{T} \vdash n$ with this inference system but $\mathsf{T} \nvdash n$ with the inference system of the previous exercise
2. Show that this inference system is not local
3. Provide an algorithm to decide the intruder deduction problem for this inference system
   Hint: you can "adapt" the definition of locality with an extended notion of subterms: the set $\mathsf{st}_{\mathsf{ext}}(t)$ is the smallest set such that
   - $\mathsf{st}(t) \subseteq \mathsf{st}_{\mathsf{ext}}(t)$
   - if $\mathsf{sign}(\mathsf{blind}(x,y),z) \in \mathsf{st}_{\mathsf{ext}}$ then $\mathsf{sign}(x,z) \in \mathsf{st}_{\mathsf{ext}}(t)$