Algorithmic aspects of cryptographic protocols

Sándor Vályi, Péter Takács, József Ködmön

Tatracrypt 2007, Smolenice, Slovakia

Cryptography, protocols and verification

- Make impossible to break secrecy of communication by detecting and exploiting flaws in protocols for communication (even in presence of perfect cryptography)

- Mathematical proofs for secrecy

  - from occasional ideas

  - through manual proof searching in formalized environments

  - to automated verification systems

Protocol specifications involving time

- time stamps
- time-released secrets
- time restricted answer for authentication etc.

Specification languages for time-dependent protocols I.

- Finite-state systems with time constraints
  - propositional temporal logic with time constraints
  - real-time graphical temporal logic
  - timed automata (finite , Büchi , tree)

Specification languages for time-dependent protocols II.

- For systems of arbitrary complexity (unbounded number of processes, sessions or generated nounces – *only a subjective selection*)

  - Theory of communicating sequential processes, spi-calculus (Dolev-Yao, Evans-Schneider, Huima, Amadio et. al., Boreale, Fiore-Abadi)

  - Term rewriting systems (Cervesato et al., Delzanno-Ganty)

  - Constraint solving (Comon et al., Millen-Shmatikov)

  - First-order modal logic (Coffey-Saidha, Coffey-Newe, Kudo-Mathuria, Takács) – using explicit time parameters

Decidability and related issues of protocol verification

- Validity of finite-state specifications is usually decidable
- Validity of infinite-space specifications is usually undecidable
- Undecidability techniques: simulating Turing machines or two-counter machines

Results on first-order modal logic of Coffey and Saidha

- We show that it is undecidable whether a given protocol specification is valid or not

- We also show that the language of valid protocol specifications is not even recursively enumerable if we consider models over integer time model $(\mathbf{Z}, <)$

- Finally we show that this problem is recursively enumerable over dense time model $(\mathbf{Q}, <)$

- We also provide a semantics for the axioms. (There is no available semantics in the literature.)

The first-order modal language of Coffey and Saidha *(a comprehension)*

- Object types and corresponding variables for them
  - for entities(agents) $\Sigma, \Omega, \ldots$
  - for texts (both cleartext and encrypted) $x, y, \ldots$
  - for time instances $t_1, t_2, \ldots$
- Constants are
  - $A(lice)$,$B(ob)$, AS *(Authentication server)* - entities and
  - 0 - a time instance

Relation and function symbols connecting objects

and their intended meaning

Function symbols

- $k(\Sigma)$ - public key of Σ, a text
- $k^{-1}(\Sigma)$ - private key of Σ, also a text
- $e(x, y)$ - result of encoding of x by key y, a text
- $d(x, y)$ - result of decoding of x by key y, a text

Predicate symbols

- $S(\Sigma, t, x)$ - Σ sends message x in time point t
- $R(\Sigma, t, x)$ - Σ receives message x in time point t
- $C(x, y)$ - text y is a component of text x
- $L(\Sigma, t, x)$ - Σ knows text x at time point t

Terms and formulæ of the language

We try to make exact the notions of the C-S system.

- The terms are the usual first-order terms of the given signature

- The formulae are defined inductively:

- – the atomic formulae are the usual first-order formulæ of the given signature

  – if φ and θ are formulæ, then $(\varphi \wedge \theta)$, $(\varphi \vee \theta)$, $(\varphi \rightarrow \theta)$, $\neg\varphi$ are formulæ, too

- if v is a variable and φ is a formula then $\forall v\ \varphi$ and $\exists v\ \varphi$ are formulæ, too

- if φ is a formula, x is entity term and t is a time term then $B_{\Sigma,t}\varphi$ and $K_{\Sigma,t}\varphi$ are formulæ, too

- $K_{\Sigma,t}\varphi$ is intended to mean that Σ knows the truth of φ at the moment t while $B_{\Sigma,t}\varphi$ reads as Σ believes in the truth of φ at the moment t

- K and B are modal operators with quantifiable parameters

There is no known description of the semantics for this first-order modal logic – despite that to give a semantics is not a totally trivial task. We begin with this.

Semantics – models for the language

As usual, we do not intend to throw out models by semantic restrictions, we let this job to the axioms. To interpet the above language over a time flow $(T, <)$ we have to specify the followings:

- *interpretations for the domains*
  - a finite set of agents, let us denote it by $Agents$
  - the set of possible messages, without loss of generality $\{0, 1\}^*$
  - the time flow is fixed to $(T, <)$

- interpreting functions for k, k^{-1}, e and d,

  - for example the interpretation of e is the intended encryption function $e^{\mathcal{I}}$ from $\{0,1\}^*$ to $\{0,1\}^*$
    Notice: any such function is an interpretation, the coming axioms will restrict later the possible interpretations and will specify what do we want from a perfect cryptographic encoding function

- interpreting relations for S, R, C and L, for example
  - the interpretation of L is the *text knowledge description* it is a function $L^{\mathcal{I}} : Agents \times T \rightarrow P(\{0,1\}^*)$
  - the interpretation of S is a relation $S^{\mathcal{I}} \subseteq Agents \times T \times \{0,1\}^*$
  - similar for $R^{\mathcal{I}}$
  - we do not take care here for what does a component of a text mean, the only relevant property will be governed by a corresponding axiom

Till this point, there is no difference with a usual first-order interpretion.

- *interpretations for knowledge/belief description*
  they are functions $K^{\mathcal{I}}, B^{\mathcal{I}} : Agents \times T \rightarrow P(Valuated\_Formulae)$, where the set $Valuated\_Formulae$ consists of formulæ equipped with valuations for the corresponding parameters.

Further semantic notions: valuation, term value, truth value

- The notion of *valuation* and *value of a term* does not differ with the classical first-order analogues. The value of a term t valuated by v is denoted by $|t|_v$.

- The definition of *semantic (truth) values* of valuated formulæ is to extend by two clauses:

  - $\|K_{\Sigma,t}\varphi\|^{\mathcal{I}}_v = (\varphi \in K^{\mathcal{I}}(|\Sigma|_v, |t|_v))$

  - $\|B_{\Sigma,t}\varphi\|^{\mathcal{I}}_v = (\varphi \in B^{\mathcal{I}}(|\Sigma|_v, |t|_v))$

Satisfaction, consequence

- If $\mathcal{I}$ is an interpretation, φ is a formula and v is a valuation then $\mathcal{I} \models \varphi v$ denotes that $\|\varphi\|_v^{\mathcal{I}}$ is $TRUE$.

- If Γ is a set of formulæ and φ is a formula then $\Gamma \models_{(T,<)} \varphi$ means that for all interpretation $\mathcal{I}$ with time component $(T,<)$ and for all valuation v, if for all $\psi \in \Gamma$: $\mathcal{I} \models \psi v$ then $\mathcal{I} \models \varphi v$

Axioms of Coffey and Saidha

They restrict the allowed class of interpretations. They specify the expected properties of the language components of the given first-order modal logic.

Initial assumptions

They describes the initial circumstances around the communication in the given protocol.

Protocol goals

They give what conditions we want to satisfy by the protocol communication

What we can learn from the paper of Coffey and Saidha?
Protocol validity problems are the same as consequence problems

$$Logical\_axioms + Nonlogical\_axioms + Initialisation \models_{(Z,<)} Goals$$

in the described first-order modal logic.

As usual, the problem of valid unbounded protocol specifications is undecidable. We state more – if we consider the protocols over integer time scale $(\mathbf{Z}, <)$.

Theorem 1. The language of valid protocol specifications over the integer time is not recursively enumerable.

It implies that no general proof searching system can be defined, e.g. the axiom system of Coffey and Saidha is not complete for this semantics. A possible way out is the following.

Theorem 2. The language of valid protocol specifications over the rational time is recursively enumerable.

Proof idea for Thm. 1.

We can interpret the first-order temporal theory over the time flow $(\mathbf{Z}, <)$ with a unary signature into the above defined first-order modal theories. The first is not recursively enumerable. (Hodkinson, Vályi)

Proof idea for Thm. 2.

We can translate the above defined first-order modal formulæ into the first-order temporal formulæ over the time flow $(\mathbf{Q}, <)$ with an arbitrary signature - and the last is recursively enumerable. (Reynolds,Vályi)

Thank you for your attention.