Formal Techniques – 2022-06-21

Exercise 1. *Informally describe the four CTL formulae* $\mathsf{AF}\phi, \mathsf{AG}\phi, \mathsf{EF}\phi, \mathsf{EG}\phi$ *(where* ϕ *is atomic), providing for each one a brief description (1-3 lines), and one example where it holds.*

Exercise 2. *Formalize the following cryptographic protocol fragment using the* applied-pi *notation.*
Initially, Alice knows symmetric keys $\mathsf{k1}, \mathsf{k2}$*. Another symmetric key,* $\mathsf{k3}$*, is shared between Alice and Bob.*
1) Alice encrypts $\mathsf{k1}$ *with* $\mathsf{k2}$*, and sends it to Bob. She also randomly generates a nonce* N*, and sends it to Bob.*
2) Bob randomly generates a nonce M*, and sends the pair* (N, M) *to Alice, after encrypting it with* $\mathsf{k3}$*.*
3) Alice checks that the received pair indeed contains her nonce N*. If that is the case, she recovers* M *and encrypts* $\mathsf{k2}$ *using* M *(using it as a symmetric key), sending such encryption to Bob.*
4) Bob then recovers $\mathsf{k2}$ *and* $\mathsf{k1}$*, and sends to Alice the message* ok *encrypted with* $\mathsf{k1}$*.*

Exercise 3. *Consider the following tree automaton*

$$\mathsf{@a} \to \mathsf{dec}(\mathsf{@a}, \mathsf{@a}), \mathsf{enc}(\mathsf{@b}, \mathsf{@c}), \mathsf{k2} \qquad \mathsf{@b} \to \mathsf{enc}(\mathsf{@d}, \mathsf{@e})$$
$$\mathsf{@c} \to \mathsf{enc}(\mathsf{@g}, \mathsf{@f}), \mathsf{dec}(\mathsf{@c}, \mathsf{@c}), \mathsf{k3} \quad \mathsf{@d} \to \mathsf{m1} \quad \mathsf{@e} \to \mathsf{k2} \quad \mathsf{@f} \to \mathsf{k3}$$
$$\mathsf{@g} \to \mathsf{k1}, \mathsf{k2}, \mathsf{m2}$$

and the rewriting rule

$$\mathsf{dec}(\mathsf{enc}(M, K), K) \Rightarrow M$$

Apply the completion algorithm to the above automaton, building an over-approximation for the languages associated to its states which is closed under rewriting. Assuming $\mathsf{@a}$ *models the set of messages being exchanged over a public channel, state what can be concluded about the secrecy of* $\mathsf{m1}, \mathsf{m2}$*.*

Exercise 4. *Formally prove the following formula exploiting the Curry-Howard isomorphism.*

$$\forall p, q : \mathsf{Prop}.\ [(p \to q) \to (p \to (p \wedge q))] \wedge [(p \to (p \wedge q)) \to (p \to q)]$$

Exercise 5. *Let* $\mathcal{A}$ *be a CL, and consider the following two definitions:*

- $\mathcal{A}$ *satisfies the* ascending chain condition *(ACC) if and only if there is no infinite sequence of strictly increasing elements* $a_0 \sqsubset a_1 \sqsubset \cdots$ *with* $a_0, a_1, \ldots \in \mathcal{A}$*.*
- *An element* x *in* $\mathcal{A}$ *is* compact *if and only if for each* $B \subseteq \mathcal{A}$ *such that* $x \sqsubseteq \bigsqcup B$ *there exists a* $\underline{\textit{finite}}$ $C \subseteq B$ *such that* $x \sqsubseteq \bigsqcup C$*.*

Prove that $\mathcal{A}$ *satisfies ACC if and only if every* $x \in \mathcal{A}$ *is compact.*