Short introductions by example to Coq and provable security

Jaime Gaspar

Universitat Rovira i Virgili, Department of Computer Engineering and Mathematics, UNESCO Chair in Data Privacy, Av. Països Catalans 26, E-43007 Tarragona, Catalonia, `jaime.gaspar@urv.cat`. Centro de Matemática e Aplicações (CMA), FCT, UNL. Financially supported by the Martí Franquès Research Fellowship Programme grant number 2013PMF-PIPF-24 of the Universitat Rovira i Virgili. The author is with the UNESCO Chair in Data Privacy, but the views expressed in this talk are his own and do not commit UNESCO.

Resumo: In this talk we give very elementary introductions, by means of very simple examples, to two topics in the intersection of mathematics, science and technology: *Coq* and *provable security*. We treat the topics separately and we keep the talk short, simple and sweet.

Coq It is a proof assistant: computer programs that help mathematicians to prove theorems and to formally verify the correctness of proofs, and are today one of the more exciting areas in the intersection of mathematics and computer science. We introduce Coq by the following example: the proofs of

- if $\leq$ is a non-strict partial order, then $<$ defined by $x < y \Leftrightarrow x \leq y \wedge x \neq y$ is a strict partial order;
- if $<$ is a strict partial order, then $\leq$ defined by $x \leq y \Leftrightarrow x < y \vee x = y$ is a non-strict partial order.

Provable security It is an area in cryptography where we rigorously

- define a *cipher*;
- define a *notion of security*;
- prove that the *cipher* is *secure*;

and so it addresses one of today's most important questions: are our ciphers secure? We introduce provable security by the following example:

$$\begin{aligned} \text{cipher} &= \text{one-time pad}, \\ \text{notion of security} &= \text{perfect secrecy}. \end{aligned}$$

Palavras-chave: Coq; proof assistant; formal verification; partial order; provable security; cryptography; one-time pad; perfect secrecy.