Provable Security – the Future or a Myth?

Karthik Bhargavan, Microsoft Research, Cambridge, UK
Peter Hellekalek, pLab, University of Salzburg, Austria
Alexandre Stervinou, RSA Security, Europe

moderator: Tomáš Rosa, eBanka

Provable Security

- Ideally: We prove that a mechanism is secure.
- But, it depends on:
  - Under what conditions the proof holds.
  - What we mean by the term “secure”.
  - How much heuristic the proof is.

For instance…

- RSAES-OAEP is provably secure under IND-CCA_2 model.
- However:
  - 2001: Manger presented a practical attack.
  - 2002: Klíma and Rosa presented a practical attack.
- What was wrong?
  - The conditions.
- Is RSA-OAEP bad?
  - Certainly not. However, the proof is not enough in itself.

Convincing Security

- The aim: To convince architects to use that mechanism.
  - It must be usable, manageable, auditable, sellable, …, and, of course, secure.

Is Provable Security also Convincing?

- It is a question of:
  - Under what conditions the proof holds.
  - What we mean by the term “secure”.
  - How much heuristic the proof is.
- Problem:
  - The more convincing the conditions and definitions are, the more heuristic the proof is.

The Future or a Myth?

- Two viewpoints:
  1. Theory
     - Provable security as a research tool.
  2. Practice
     - Provable security as a platform for the convincing security.