A composable computational soundness notion

Véronique Cortier[1] and Bogdan Warinschi[2]

[1] CNRS, Loria, France
[2] Bristol University

Computational soundness results show that under certain conditions it is possible to conclude computational security whenever symbolic security holds. Unfortunately, each soundness result is usually established for some set of cryptographic primitives and extending the result to encompass new primitives typically requires redoing most of the work.

We define *deduction soundness*, a computational soundness notion that directly captures the idea that a computational adversary does not have any more power than a symbolic adversary. Our definition, by default, considers the use of the primitives in the presence of other, unspecified functions. As a result we show that our notion is amenable to modular extensions. We demonstate that an implementation that is deduction sound for some set of primitives can be extended to also include asymmetric encryption and public data-structures (e.g. pairings or list), while preserving deduction soundness and without repeating the original proof effort. To the best of our knowledge this is the first modular computational soundness result.

Furthermore, our notion of soundness only concerns the primitives themselves in a way that is independent of any protocol specification language. Nevertheless, we show that deduction soundness leads to computational soundness for languages (or protocols) that satisfy a so called *commutation property*.