Secure CCP: A Declarative Framework for Security

Security has become a serious challenge involving several disciplines of Computer Science. In particular, there has been a growing interest in the analysis of security protocols. One promising approach is the use of process calculi, formalisms that model communicating processes. The results are so far encouraging although most remains to be done.

Process calculi for security have strong similarities with CCP:

- Several process calculi variants are all operationally defined in terms of configurations containing information which can only increase during evolution. This is akin to the notion of monotonic store, central to CCP.
- Also, several process calculi variants are parametric in the underlying logic much like CCP is parametric in an underlying constraint system.

The notion of unification, which has been shown useful for the symbolic execution of protocols, is primitive (and more general) in CCP.

Our project Secure CCP (SCCP) aims at advancing both the theory and tools of CCP for analyzing and programming security protocols.

Novelty
To our best knowledge, there is no work on Security that takes advantage of the reasoning techniques of CCP.

Expected outcome
To advance the CCP theory to deal with new challenging concepts from Security and produce a specification language and tools to model and automatically verify security protocols.

Approach
To give a CCP account of a representative calculus for security protocols. We will use CCP constraint systems to represent a logic to reason about the information an attacker can deduce from the information accumulated in the store.