BSc project proposal: Composition of Cryptographic Systems

Student: Pieter Rogaar (Leiden University); Advisor: Dennis Hofheinz (CWI)

What does it mean for a cryptographic system (e.g., an encryption system, or a large internet banking protocol) to be *secure*? Different notions have been suggested, some of them specifically geared towards capturing security of a concrete cryptographic task, some of them very generic and abstract. In the current project, we are taking a closer look at generic and abstract security notions. In particular, such security notions are attractive because they allow to treat the security of different systems, possibly even for different cryptographic tasks, in a unified way.

More concretely, we investigate the effect of *composition* on the security of cryptographic systems. By composition, we mean combining different cryptographic building blocks into one larger system. Of course, the question arises how the security of this composed system is connected to the security of its smaller components. Does the combination of, say, two secure systems necessarily result in a secure system? When and under which security definitions does this hold?

Technically, we consider two established generic and abstract notions of security for cryptographic systems: Universal Composability [Can01] (UC) and Indifferentiability [MRH04]. UC is geared towards analyzing complex multi-party protocols in a modular fashion: all building blocks of a large protocol are analyzed separately and then put together; a powerful *composition theorem* guarantees that the composed protocol inherits the security of the building blocks. On the other hand, the Indifferentiability framework is technically very similar, but aims at analyzing smaller, non-interactive cryptographic primitives. However, while UC is known for its powerful composition theorem, the situation regarding composed protocols is less clear for Indifferentiability.

The technical contribution of this project will be to transport the strong compositional guarantees of UC to the Indifferentiability setting. In particular, this will require understanding and using the technical tools common to both frameworks. The work will build up an understanding of general cryptographic techniques, as well as techniques typical for the analysis of composed systems.

References

[Can01] Ran Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *42th Annual Symposium on Foundations of Computer Science, Proceedings of FOCS 2001*, pages 136–145. IEEE Computer Society, 2001.

[MRH04] Ueli Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In Moni Naor, editor, *Theory of Cryptography, Proceedings of TCC 2004*, number 2951 in Lecture Notes in Computer Science, pages 21–39. Springer-Verlag, 2004.