A simple model of polynomial time UC

Dennis Hofheinz[1], Jörn Müller-Quade[2], and Dominique Unruh[2]

[1] CWI, Amsterdam, `Dennis.Hofheinz@cwi.nl`
[2] IAKS, Universität Karlsruhe, `{muellerq,unruh}@ira.uka.de`

Traditionally, simulation-based security, such as UC and Reactive Simulatability, defines polynomial-time machines as follows: There is a polynomial p, s.t. the running time is bounded in $p(k)$, where k is the security parameter. However, it turned out that this definition is too restrictive for many applications. Unless we fix *arbitrary* bounds on the communication, even a party that just forwards its input to another party is not polynomially bounded in the security parameter, but only *in the length of its inputs*.

Recently, it has been tried to extend simulation-based security to allow for protocols of this nature. However, it turns out that it is difficult to find a suitable definition while still preserving important properties of the security model like composability. Therefore, the security definitions are either quite complicated (as in [2]), or some additional requirements have to be imposed on the protocols (in [1], the protocol output must be strictly shorter than its inputs, in [3] certain acyclicity conditions have to apply to the "flow of running time" in the protocol).

We present a new definition of UC that can be applied to protocols satisfying the following general definition of polynomial time:

Definition. *A protocol π is* reactively polynomial*, if for any (strictly) polynomial-time machine T (the tester), the network $T+\pi$ (T running and communicating with π) runs in polynomial-time with overwhelming probability.*

This definition is probably the weakest possible reasonable definition of polynomial-time.

Our security definition then is the following:

Definition. *A reactively polynomial protocol π* securely implements *a reactively polynomial functionality $\mathcal{F}$, if for any adversary $\mathcal{A}$ s.t. $\mathcal{A}+\pi$ is reactively polynomial, there is a simulator $\mathcal{S}$ s.t. $\mathcal{S}+\mathcal{F}$ is reactively polynomial, s.t. for every (strictly) polynomial environment $\mathcal{Z}$, it holds that:*

The outputs of $\mathcal{Z}$ in an execution of $\pi+\mathcal{A}+\mathcal{Z}$ and of $\mathcal{F}+\mathcal{S}+\mathcal{Z}$ are computationally indistinguishable.

We show that this definition is endowed with a composition theorem:

Theorem. *By σ^π we denote the protocol σ calling an instance of π, and define $\sigma^{\mathcal{F}}$ analogously. Let π securely implement $\mathcal{F}$. Let σ be a protocol, s.t. σ^π and $\sigma^{\mathcal{F}}$ are reactively polynomial.*

Then σ^π securely realises $\sigma^{\mathcal{F}}$.

Note, however, that this composition theorem only allows to replace one instance of $\mathcal{F}$ at a time. Whether our definition allows for concurrent composition (replacing many copies of $\mathcal{F}$ simultaneously), is currently being investigated.

Furthermore, our security model has a complete dummy adversary, i.e., it is only necessary to prove security against the adversary that simply forwards communication between environment and protocol.

[1] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. IACR ePrint 2000/067, December 2005.

[2] Dennis Hofheinz, Jörn Müller-Quade, and Dominique Unruh. Polynomial runtime in simulatability definitions. In *18th IEEE Computer Security Foundations Workshop, Proceedings of CSFW 2005*, pages 156–169. IEEE Computer Society, 2005.

[3] Ralf Küsters. Simulation-based security with inexhaustible interactive turing machines. IACR ePrint 2006/151.