Title: **On the Relationships between Notions of Simulation-Based Security**

Author: **Küsters, R., Datta, A., Mitchell, J.C. and Ramanathan, A**

Published in: *Journal of Cryptology, Lecture Notes in Comput. Sci.*, **21**, 492–546, (2008)

Review by: Mario Forcinito

In analyzing the security of cryptographic protocols, the standard procedure is to compare the functionality of the real protocol against the protocol performed by a set of idealized trusted parties, each performing a defined function and with known security properties (see [1] for a more detailed account).

Several security notions have been proposed by researchers to conduct the analysis of cryptographic protocols such as Universal Composability, Reactive Simulatability, Black-Box Simulatability.

This paper clarifies the relationships between the various security notions, that can be obtained by the different combinations between entities (environment, real/ideal adversary, simulator, real/ideal protocol).

A crucial issue for the relationships between the security notions identified by the authors is the ability to define a forwarding process.

Although intuition tell us that a forwarder can be placed between two processes two processes without changing the overall behavior of the system, the authors found that this can violate some complexity bounds with the consequent loss of some messages. This is very important in the context of this paper because some proofs require the existence of forwarders that cannot be exhausted.

The authors give complete and rigorous proofs that uncover several non-trivial aspects of the equivalence between security notions.

See also:

1. Hofheinz, D. and Unruh, D. Simulatable Security and Polynomially Bounded Concurrent Composability, available online at
http://homepages.cwi.nl/∼hofheinz/pdf/conccomp.pdf

2. Canetti, R., Universally composable security: a new paradigm for cryptographic protocols. Technical report, Cryptology ePrint Archive, December 2005. Available online at
http://eprint.iacr.org/2000/067.ps