Cryptology ePrint Archive: Report 2011/355

Comparing UC Security Variants

Oana Ciobotaru

Abstract: In this work we investigate the relations among various security notions. More precisely, we present a separation result between two variants of UC security defi nition: 1-bit specialized simulator UC security and specialized simulator UC security. This solves an open question from [Lindell,2003] and comes in contrast with the well known equivalence result between 1-bit UC security and UC security. We also give a notion of weak security and we show that the induced weak security under 1-bounded concurrent general composition is equivalent to 1-bit specialized simulator UC security. As a consequence, we obtain that our notion of weak security and the notion of stand-alone security are not equivalent.

Category / Keywords: foundations / weak security; composability; 1-bit specialized simulator UC security; time-lock puzzles

Date: received 1 Jul 2011, last revised 19 Jul 2011

Contact author: ociobota at mpi-inf mpg de