

# Cryptology ePrint Archive: Report 2011/303

## GNUC: A New Universal Composability Framework

*Dennis Hofheinz and Victor Shoup*

**Abstract:** We put forward a framework for the modular design and analysis of multi-party protocols. Our framework is called "GNUC" (with the recursive meaning "GNUC's Not UC"), already alluding to the similarity to Canetti's Universal Composability (UC) framework. In particular, like UC, we offer a universal composition theorem, as well as a theorem for composing protocols with joint state. We deviate from UC in several important aspects. Specifically, we have a rather different view than UC on the structuring of protocols, on the notion of polynomial-time protocols and attacks, and on corruptions. We will motivate our definitional choices by explaining why the definitions in the UC framework are problematic, and how we overcome these problems. Our goal is to make offer a framework that is largely compatible with UC, such that previous results formulated in UC carry over to GNUC with minimal changes. We exemplify this by giving explicit formulations for several important protocol tasks, including authenticated and secure communication, as well as commitment and secure function evaluation.

**Category / Keywords:** foundations / protocols, composability

**Date:** received 6 Jun 2011

**Contact author:** shoup at cs nyu edu

**Available formats:** [PDF](#) | [BibTeX Citation](#)

**Version:** 20110608:113703 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]