Cryptology ePrint Archive: Report 2011/339

Careful with Composition: Limitations of Indifferentiability and Universal Composability

Thomas Ristenpart and Hovav Shacham and Thomas Shrimpton

Abstract: We exhibit a hash-based storage auditing scheme which is provably secure in the random-oracle model (ROM), but easily broken when one instead uses typical indifferentiable hash constructions. This contradicts the widely accepted belief that the indifferentiability composition theorem applies to any cryptosystem. We characterize the uncovered limitation of the indifferentiability framework by show- ing that the formalizations used thus far implicitly exclude security notions captured by experiments that have multiple, disjoint adversarial stages. Examples include deterministic public-key encryption (PKE), password-based cryptography, hash function nonmalleability, key-dependent message security, and more. We formalize a stronger notion, reset indifferentiability, that enables an indifferentiability- style composition theorem covering such multi-stage security notions, but then show that practical hash constructions cannot be reset indifferentiable. We discuss how these limitations also affect the universal composability framework. We finish by showing the chosen-distribution attack security (which requires a multi-stage game) of some important public-key encryption schemes built using a hash construction paradigm introduced by Dodis, Ristenpart, and Shrimpton.

Category / Keywords:

Publication Info: A preliminary version of this paper was published under the title "Careful with Composition: Limitations of the Indifferentiability Framework" at Eurocrypt 2011

Date: received 22 Jun 2011

Contact author: rist at cs wisc edu