Cryptology ePrint Archive: Report 2013/002

Generalized (Identity-Based) Hash Proof System and Its Applications

Yu Chen and Zongyang Zhang and Dongdai Lin and Zhenfu Cao

Abstract: In this work, we generalize the paradigm of hash proof system (HPS) proposed by Cramer and Shoup [CS02]. In the central of our generalization, we lift subset membership problem to distribution distinguish problem. Our generalized HPS clarifies and encompass all the known public-key encryption (PKE) schemes that essentially implement the idea of hash proof system. Moreover, besides existing smoothness property, we introduce an additional property named anonymity for HPS. As a natural application, we consider anonymity for PKE in the presence of key-leakage, and provide a generic construction of leakage-resilient anonymous PKE from anonymous HPS. We then extend our generalization to the identity-based setting. Concretely, we generalize the paradigm of identity-based hash proof system (IB-HPS) proposed by Boneh et al. [BGH07] and Alwen et al. [ADN+ 10], and introduce anonymity for it. As an interesting application of anonymous IB-HPS, we consider security for public-key encryption with keyword search (PEKS) in the presence of token-leakage, and provide a generic construction of leakage-resilient secure PEKS from leakage-resilient anonymous IBE, which in turn is based on anonymous IB-HPS.

Category / Keywords: (identity-based) hash proof system, leakage-resilience, anonymity, public-key encryption with keyword search

Publication Info: An extended abstract of this paper has been accepted by Provsec 2012 entitled "Anonymous Identity-Based Hash Proof System and Its Applications". This is the full version with many newly added materials.

Date: received 4 Jan 2013, last revised 4 Jan 2013

Contact author: cycosmic at gmail com

Available formats: PDF | BibTeX Citation

Note: Compared to the conference version, this version presents the generalization of (IB)-HPS, and proposes