Cryptology ePrint Archive: Report 2011/209

Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting

Zvika Brakerski and Gil Segev

Abstract: Deterministic public-key encryption, introduced by Bellare, Boldyreva, and O'Neill (CRYPTO '07), provides an alternative to randomized public-key encryption in various scenarios where the latter exhibits inherent drawbacks. A deterministic encryption algorithm, however, cannot satisfy any meaningful notion of security when the plaintext is distributed over a small set. Bellare et al. addressed this difficulty by requiring semantic security to hold only when the plaintext has high min-entropy from the adversary's point of view.

In many applications, however, an adversary may obtain auxiliary information that is related to the plaintext. Specifically, when deterministic encryption is used as a building block of a larger system, it is rather likely that plaintexts do not have high min-entropy from the adversary's point of view. In such cases, the framework of Bellare et al. might fall short from providing robust security guarantees.

We formalize a framework for studying the security of deterministic public-key encryption schemes with respect to auxiliary inputs. Given the trivial requirement that the plaintext should not be efficiently recoverable from the auxiliary input, we focus on {\em hard-to-invert} auxiliary inputs. Within this framework, we propose two schemes: the first is based on the decisional Diffie-Hellman (and, more generally, on the d-linear) assumption, and the second is based on a rather general class of subgroup indistinguishability assumptions (including, in particular, quadratic residuosity and Paillier's composite residuosity). Our schemes are secure with respect to any auxiliary input that is subexponentially hard to invert (assuming the {\em standard} hardness of the underlying computational assumptions). In addition, our first scheme is secure even in the multi-user setting where related plaintexts may be encrypted under multiple public keys. Constructing a scheme that is secure in the multi-user setting (even without considering auxiliary inputs) was identified by Bellare et al. as an important open problem.

Category / Keywords: public-key cryptography / deterministic encryption, auxiliary inputs, composable security

Publication Info: CRYPTO 2011

Date: received 1 May 2011, last revised 30 Aug 2011

Contact author: gil segev at microsoft com

Available formats: PDF | BibTeX Citation

Version: 20110830:162932 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]