

Cryptology ePrint Archive: Report 2011/230

All-But-Many Lossy Trapdoor Functions

Dennis Hofheinz

Abstract: We put forward a generalization of lossy trapdoor functions (LTFs). Namely, all-but-many lossy trapdoor functions (ABM-LTFs) are LTFs that are parametrized with tags. Each tag can either be injective or lossy, which leads to an invertible or a lossy function. The interesting property of ABM-LTFs is that it is possible to generate an arbitrary number of lossy tags by means of a special trapdoor, while it is not feasible to produce lossy tags without this trapdoor.

Our definition and construction can be seen as generalizations of all-but-one LTFs (due to Peikert and Waters) and all-but-N LTFs (due to Hemenway et al.). However, to achieve ABM-LTFs (and thus a number of lossy tags which is not bounded by any polynomial), we have to employ some new tricks. Concretely, we give two constructions that employ "disguised" variants of the Waters, resp. Boneh-Boyen signature schemes to make the generation of lossy tags hard without trapdoor. In a nutshell, lossy tags simply correspond to valid signatures. At the same time, tags are disguised (i.e., suitably blinded) to keep lossy tags indistinguishable from injective tags.

ABM-LTFs are useful in settings in which there are a polynomial number of adversarial challenges (e.g., challenge ciphertexts). Specifically, building on work by Hemenway et al., we show that ABM-LTFs can be used to achieve selective opening security against chosen-ciphertext attacks. One of our ABM-LTF constructions thus yields the first SO-CCA secure encryption scheme with compact ciphertexts ($O(1)$ group elements) whose efficiency does not depend on the number of challenges. Our second ABM-LTF construction yields an IND-CCA (and in fact SO-CCA) secure encryption scheme whose security reduction is independent of the number of challenges and decryption queries.

Category / Keywords: public-key cryptography / lossy trapdoor functions, public-key encryption, selective opening attacks

Date: received 10 May 2011, last revised 30 Dec 2011

Contact author: Dennis Hofheinz at kit.edu

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

Note: Update (2011-07-29): rearranged, fixed a small bug in proof of DCR-based construction, fixed typos. Update (2011-10-10): improved lossiness analysis of DCR-based construction. (Lossiness actually already follows in rings \mathbb{Z}_N^s for $s \geq 3$.) Update (2011-12-30): incorporated referee comments.

Version: 20111230:093405 ([All versions of this report](#))

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

[[Cryptology ePrint archive](#)]