

Cryptology ePrint Archive: Report 2011/559

Instantiability of RSA-OAEP under Chosen-Plaintext Attack

Eike Kiltz and Adam O'Neill and Adam Smith

Abstract: We show that the widely deployed RSA-OAEP encryption scheme of Bellare and Rogaway (Eurocrypt 1994), which combines RSA with two rounds of an underlying Feistel network whose hash (i.e., round) functions are modeled as random oracles, meets indistinguishability under chosen-plaintext attack (IND-CPA) in the standard model based on simple, non-interactive, and non-interdependent assumptions on RSA and the hash functions. To prove this, we first give a result on a more general notion called "padding-based" encryption, saying that such a scheme is IND-CPA if (1) its underlying padding transform satisfies a "fooling" condition against small-range distinguishers on a class of high-entropy input distributions, and (2) its trapdoor permutation is sufficiently lossy as defined by Peikert and Waters (STOC 2008). We then show that the first round of OAEP satisfies condition (1) if its hash function is ϵ -wise independent for appropriate ϵ and that RSA satisfies condition (2) under the Φ -Hiding Assumption of Cachin et al. (Eurocrypt 1999). This appears to be the first non-trivial positive result about the instantiability of RSA-OAEP. In particular, it increases our confidence that chosen-plaintext attacks are unlikely to be found against the scheme. In contrast, RSA-OAEP's predecessor in PKCS #1 v1.5 was shown to be vulnerable to such attacks by Coron et al. (Eurocrypt 2000).

Category / Keywords: public-key cryptography / RSA, OAEP, padding-based encryption, lossy trapdoor functions, leftover hash lemma, standard model

Publication Info: CRYPTO 2010

Date: received 13 Oct 2011

Contact author: amoneill at bu edu

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

Note: This is the full version.

Version: 20111017:194114 ([All versions of this report](#))

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

[[Cryptology ePrint archive](#)]