

OAEP Reconsidered

Victor Shoup, *IBM Zurich Research Lab, Sumerstr. 4, 8803 Rschlikon, Switzerland.*

We will begin with some recalls about security against adaptative chosen cyphertext attack, random oracle models, and one-way trapdoor permutations and, of course, about the OAEP scheme.

We will explain through an example how the technique proof of OAEP fails when we have an algorithm that can invert the one-way trapdoor permutation. Then we are going to show that there exists an oracle relative to which OAEP is insecure ; that is, there exists no "black box" security reduction for OAEP. That will allow us to build an adversary who can break the cryptosystem in such a way that no simulator given black box access to the adversary and its random oracle queries can use our adversary to get any information on a plaintext deduced from a given ciphertext.

OAEP+ is a slightly different version of OAEP, which is claimed to be essentially just as efficient as the standard scheme. The idea was to get a tighter security reduction, using data-dependent redundancy in a given way, instead of using data-independent redundancy. We will introduce this new scheme, and explain why it can be claimed secure against adaptative chosen ciphertext attack in the random oracle model and supposing that the underlying trapdoor permutation scheme is one way.

In the original article, Victor Shoup, claims that OAEP' is secure, but theorems which are used for proving that OAEP is not secure hold also for OAEP'. We show that for some specific trapdoor function, RSA with exponent 3 for example, OAEP scheme is provable secure. In fact, RSA-OAEP is provable secure for any exponant. In the article : "What Hashes Make RSA-OAEP secure?" (08/08/2007) Daniel.R.L.Brown, shows that there exist pathological hash function such that RSA-OAEP is insecure.

Unfortunately, the determination of which cryptographic properties are mandatory for RSA-OAEP security, is not complete. We've not found articles which exhibit xor-malleable trapdoor function.

1 Plan

1.1 Introduction

1.2 Recall

1.3 OAEP is not secure

1.3.1 Example

1.3.2 Formal evidence

1.4 OAEP+

1.4.1 Introduction

1.4.2 CCA2 secure

1.5 Further observations

1.5.1 OAEP'

1.5.2 RSA-OAEP