# Cryptology ePrint Archive: Report 2011/678

**On definitions of selective opening security**

*Florian Böhl and Dennis Hofheinz and Daniel Kraschewski*

**Abstract:** Assume that an adversary observes many ciphertexts, and may then ask for openings, i.e. the plaintext and the randomness used for encryption, of some of them. Do the unopened ciphertexts remain secure? There are several ways to formalize this question, and the ensuing security notions are not known to be implied by standard notions of encryption security. In this work, we relate the two existing flavors of selective opening security. Our main result is that indistinguishability-based selective opening security and simulation-based selective opening security do not imply each other.

We show our claims by counterexamples. Concretely, we construct two public-key encryption schemes. One scheme is secure under selective openings in a simulation-based sense, but not in an indistinguishability-based sense. The other scheme is secure in an indistinguishability-based sense, but not in a simulation-based sense.

Our results settle an open question of Bellare et al. (Eurocrypt 2009). Also, taken together with known results about selective opening secure encryption, we get an almost complete picture how the two flavors of selective opening security relate to standard security notions.

**Category / Keywords:** public-key cryptography / security definitions, selective opening security, public-key encryption

**Publication Info:** Full version of PKC 2012 paper

**Date:** received 15 Dec 2011, last revised 4 Apr 2012

**Contact author:** florian boehl at kit edu, dennis hofheinz@kit edu, daniel kraschewski@kit edu