Cryptology ePrint Archive: Report 2013/831

Provable Security Proofs and their Interpretation in the Real World

Vikram Singh

Abstract: This paper analyses provable security proofs, using the EDL signature scheme as its case study, and interprets their bene fits and drawbacks when applied to the real world.

Provable security has been an area of contention. Some, such as Koblitz and Menezes, give little credit to the potential extra security provided and argue that it is a distracting goal. However, others believe that an algorithm with a security proof is superior to one without it, and are prepared to accept the impact to performance that their use might involve. Goldreich has been notable for his defence of the security proof, and for his opposition to the view of Koblitz and Menezes.

This paper is designed to help the reader make their own decisions on security proofs. We achieve this by giving an introduction to the typical security model used, then give a description of the EDL signature scheme and its tight reduction to the CDH problem in the Random Oracle Model, then analyse the proof's assumptions, meaning, validity and overhead for real world security.

Category / Keywords: public-key cryptography / Provable Security, EDL Signature Scheme, Tight Reduction, Computational Diffie Hellman problem, Random Oracle Model

Date: received 5 Dec 2013

Contact author: vs77814 at gmail com