# Cryptology ePrint Archive: Report 2011/263

### The Computational Square-Root Exponent Problem- Revisited

*Fangguo Zhang*

**Abstract:** In this paper, we revisit the Computational Square-Root Exponent Problem (CSREP), and give a more generic condition such that CSREP is polynomial-time equivalent to the Computational Diffie-Hellman Problem (CDHP) in the group with prime order. The results obtained in this paper contain Zhang \textit{et al.}'s results at IWCC2011. We also analyze the existence of such condition. Although primes satisfying such condition are rare (compare to all primes), it can be regarded as an evidence that CSREP may be equivalent to CDHP.

**Category / Keywords:**

**Date:** received 25 May 2011, last revised 6 Jun 2011

**Contact author:** isszhfg at mail sysu edu cn

**Available formats:** PDF | BibTeX Citation

**Note:** Thanks to Prof. Steven Galbraith for bringing the paper of Roh et al to my attention. I added a short description about Roh et al.'s work at the end of Section 4.3 .

**Version:** 20110607:050311 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

---

[ Cryptology ePrint archive ]