

# Cryptology ePrint Archive: Report 2011/265

## Efficient 2-Round General Perfectly Secure Message Transmission: A Minor Correction to Yang and Desmedt's Protocol

*Qiushi Yang and Yvo Desmedt*

**Abstract:** At Asiacrypt'10, Yang and Desmedt proposed a number of perfectly secure message transmission protocols in the general adversary model. However, there is a minor flaw in the 2-round protocol in an undirected graph to transmit multiple messages. A small correction solves the problem. Here we fix the protocol and prove its security.

### Category / Keywords:

**Publication Info:** This result was originally going to appear in the full version of [\cite{YD10}](#). However, as required by some recent studies of this model, we show this correction on Cryptology ePrint Archive in advance.

**Date:** received 25 May 2011

**Contact author:** q yang at cs ucl ac uk

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

**Version:** 20110528:041553 ([All versions of this report](#))

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

---

[ [Cryptology ePrint archive](#) ]