http://eprint.iacr.org/2011/633