

# Cryptology ePrint Archive: Report 2011/205

## Group-oriented ring signature

*Chunbo Ma and Jun Ao*

**Abstract:** In this paper, we present an improved Rivest's ring signature scheme. In our scheme, the size of the signature is only related to the ring members, and the signer needs no to publish amount of random numbers. On this basis, we propose a group-oriented ring signature. In this scheme, only the person who belongs to the designated group can verify the validity of the ring signature. The security of these two schemes can be proved by using Forking Lemmas.

**Category / Keywords:** public-key cryptography / Ring signature, Group, Verification

**Date:** received 24 Apr 2011

**Contact author:** machunbo at guet edu cn

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

**Version:** 20110425:193259 ([All versions of this report](#))

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

---

[ [Cryptology ePrint archive](#) ]