

Title: **Enhanced Security Models and a Generic Construction Approach for Linkable Ring Signature**

Author: **Liu, Joseph K. & Duncan S.**

Published in: *Internat. J. Found. Comput. Sci.* 17(2006), no. **6**, 1403–1422

Review by: Mario Forcinito

The use of a linkable ring signature scheme solves the problem of a whistle-blower that wants to leak information remaining anonymous [1] and, at the same time being able to prove that two signatures were generated by the same person. In this way the leaker can prevent diversionary tactics by other members of the group that would seek to discredit the "leaks" by sending false verifiable false information using the whistle-blower name. Linkable ring signatures can also be used as a basis for a practical e-voting systems.

In this paper Liu and Wong extend their preliminary work presented in [2] by introducing a generic approach to the construction of linkable ring signature schemes, and based on this approach, construct two of such schemes. The security models are also extended and proved.

A new concept is also introduced, that of a *forced* or *mandatory* linkable signature scheme with property of *type-restricted separability*. In this type of schemes the participants have the ability to choose their keys independently as long as the keys belong to a single type of signature schemes.

1. Rivest, Shamir and Tauman, *How to leak a secret*, ASIACRYPT 2001, pp 552-565. Lecture Notes in Comp. Sci. No. 2248, Springer-Verlag.
2. Liu and Wong, *Linkable ring signatures: Security models and new schemes*, ICCSA 2005 pp 614-623. Lecture Notes in Comp. Sci. No. 3481, Springer-Verlag.