Cryptology ePrint Archive: Report 2013/182

Collusion-Resistant Domain-Specific Pseudonymous Signatures

Julien Bringer and Herve Chabanne and Alain Patey

Abstract: At ISC 2012, Bender et al. introduced the notion of domain-specific pseudonymous signatures for ID documents. With this primitive, a user can sign with domain-specific pseudonyms, that cannot be linked across domains but that are linkable in a given domain. However, their security model assumes non-collusion of malicious users, which is a strong assumption. We therefore propose improvements to their construction. Our main contribution is a new pseudonymous signature scheme based on group signatures that is collusion-resistant.

Category / Keywords: public-key cryptography / group signatures, pseudonymous signatures, electronic ID documents

Publication Info: NSS 2013

Date: received 31 Mar 2013

Contact author: alain patey at telecom-paristech fr