Scientific Research



Search Keywords, Title, Author, ISBN, ISSN

Home Journals Books Conferences News	About Us	s Jobs	
Home > Journal > Business & Economics Computer Science & Communications > IIM	Open Spec	ial Issues	
Indexing View Papers Aims & Scope Editorial Board Guideline Article Processing Charges	Published Special Issues		
IIM> Vol.2 No.9, September 2010	Special Issues Guideline		
OPEN BACCESS Improvement of Chen-Zhang-Liu's IRPB Signature Scheme	IIM Subscription		
PDF (Size: 124KB) PP. 559-562 DOI: 10.4236/iim.2010.29064	Most popular papers in IIM		
Author(s) Dezhi Gao	About IIM News		
ABSTRACT Restrictive partially blind signatures incorporate the advantages of restrictive blind signatures and partially		Frequently Asked Questions	
blind signatures, which play an important role in electronic commerce. Recently, Chen-Zhang-Liu first proposed an ID-based restrictive partially blind (IRPB) signature from bilinear pairings. Later, Hu-Huang showed that the Chen-Zhang-Liu' s scheme has a security weakness, and pointed out that their scheme does not satisfy the property of restrictiveness as they claimed. In this paper, we improve Chen-Zhang-Liu' s scheme and propose a new signature scheme from bilinear pairings. The improved scheme can resist the Hu-Huang' s attack.	Recommend to Peers		
	Recommend to Library		
	Contact Us		
KEYWORDS Cryptography, Bilinear Pairings, Restrictiveness, Partially Blind Signature, ID-Based Restrictive Partially Blind Signature	Downloads:	144,654	
	Visits:	362.633	
Cite this paper D. Gao, "Improvement of Chen-Zhang-Liu' s IRPB Signature Scheme," Intelligent Information Management, Vol. 2 No. 9, 2010, pp. 559-562. doi: 10.4236/iim.2010.29064.	Sponsors >>		
References [1] D. Chaum, " Blind Signatures for Untraceable Payments," Advances in Cryptology Crypto' 82, Springer-Verlag, Ger- many, 1982, pp. 199-203.			
 S. Brands, "Untraceable off-Line Cash in Wallets with Observers," Advances in Cryptology Crypto' 93, LNCS 773, Springer-Verlag, Germany, 1993, pp. 302-318. 			
 [3] M. Abe and E. Fujisaki, "How to Date Blind Signatures," Advances in Cryptology-Asiacrypt 1996, LNCS 1163, Springer-Verlag, Germany, 1996, pp. 244-251. 			
 [4] G. Maitland and C. Boyd, " A Provably Secure Restrictive Blind Signature Scheme," PKC' 02, LNCS 2274, Springer-Verlag, Germany, 2002, pp. 99-114. 			
[5] X. F. Chen, F. G. Zhang and S. L. Liu, " ID-Based Restrictive Partially Blind Signatures and Applications," The Journal of Systems and Software, Vol. 80, No. 2, 2007, pp. 64-71.			
[6] S. M. Chow, C. K. Hui and S. M. Yin, "Two Improved Partially Blind Signature Schemes from Bilinear Pairings," ACISP' 05, LNCS 3574, Springer-Verlag, Germany, 2005, pp. 316-328.			