Tang, Pengzhi; Chen, Renqun; Zhang, Qinglan
An analysis and improvements of a class of identity-based signcryption schemes.

Summary: Through the security analysis of two signcryption schemes, it is found that both schemes cannot meet the request for public verification and cannot defend the forge by dishonest receiver. Then two improved schemes are proposed which make up the defects of original schemes. The security analysis of the improved schemes is conducted under the random oracle mode. The result shows that the improved schemes are safer and meet the request for public verification and unforgeability.

Keywords: proxy signcryption; multi-proxy multi-signcryption; public verification; unforgeability
doi:10.3969/j.issn.1003-5060.2014.08.009