Chen, Wenbin; Li, Jin; Huang, Zhengan; Gao, Chongzhi; Yiu, Siuming; Jiang, Zoe L.
Lattice-based unidirectional infinite-use proxy re-signatures with private re-signature key.
(English) Zbl 07365384

Summary: In a proxy re-signature scheme, a semi-trusted proxy can convert Alice’s (also called as delega-tee’s) signature into Bob’s (also called as delegator’s) signature on the same message. However, the proxy itself cannot produce any signatures on behalf of either Alice or Bob. There exists some unidirectional one-use and multi-use (a message can be re-signed a polynomial number of times) proxy re-signature schemes. In some scenarios of big data, it is required to design unidirectional infinite-use (a message can be re-signed infinite number of times) proxy re-signature schemes. In this paper, we propose the first unidirectional infinite-use proxy re-signature scheme and identity-based unidirectional infinite-use proxy re-signature scheme with private re-signature keys based on lattice and prove that they are secure in the random oracle model.

MSC:
94A62 Authentication, digital signatures and secret sharing
68P25 Data encryption (aspects in computer science)

Keywords: lattice; proxy re-signature; private re-signature key; random oracle model

Full Text: DOI

References:

[9] Cash, David; Hofheinz, Dennis; Kiltz, Eike; Peikert, Chris, Bonsai tree, or how to delegate a lattice basis, (EUROCRYPT 2010 (2010)), 523-552 · Zbl 1280.94043
[13] Libert, B.; Vergnaud, D., Multi-use unidirectional proxy re-signatures, (CCS (2008), ACM), 511-520
This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.