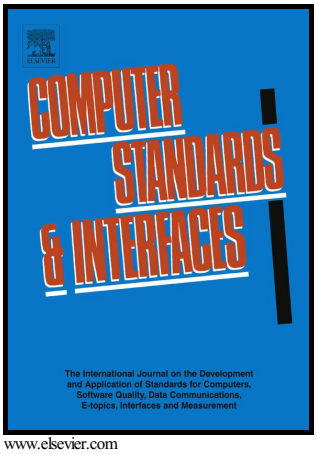

Identity-Based Provable Data Possession Revisited: Security Analysis and Generic Construction

Hongyu Liu, Yi Mu, Jining Zhao, Chunxiang Xu, Huaqun Wang, Leiting Chen, Yong Yu

PII: S0920-5489(16)30101-5
DOI: http://dx.doi.org/10.1016/j.csi.2016.09.012
Reference: CSI3144

To appear in: *Computer Standards & Interfaces*

Received date: 2 February 2016
Revised date: 18 September 2016
Accepted date: 28 September 2016

Cite this article as: Hongyu Liu, Yi Mu, Jining Zhao, Chunxiang Xu, Huaqu Wang, Leiting Chen and Yong Yu, Identity-Based Provable Data Possession Revisited: Security Analysis and Generic Construction, *Computer Standards & Interfaces,* http://dx.doi.org/10.1016/j.csi.2016.09.012

Identity-Based Provable Data Possession Revisited: Security Analysis and Generic Construction ⋆

Hongyu Liu [a,*], Yi Mu [b], Jining Zhao [a], Chunxiang Xu [a], Huaqun Wang [c], Leiting Chen [a], Yong Yu [a]

[a] *School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China*

[b] *School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia*

[c] *School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China.*

Abstract

Provable Data Possession (PDP), which enables cloud users to verify the data integrity without retrieving the entire file, is highly essential for cloud storage. Observing all the existing PDP schemes rely on the Public Key Infrastructure (PKI), Wang proposed an identity-based distributed provable data possession (ID-DPDP) scheme that can (1) eliminate the complex certificate management and (2) be applied to the multi-cloud scenario. The scheme is efficient, flexible and supports private verification, delegated verification and public verification. In this paper, we find that ID-DPDP is flawed since it fails to achieve soundness. We then fix the flaw by presenting a generic construction for identity-based PDP (ID-PDP) protocol, derived from secure digital signature schemes and traditional PDP protocols. We prove that the soundness of the generic ID-PDP construction depends on the security of the underlying PDP protocols and the signature schemes. An instance of the generic construction by utilizing a state-of-the-art PDP protocol due to Shacham and Waters and BLS short signature scheme is given. Moreover, a new ID-DPDP protocol is obtained by extending the basic ID-PDP to multiple clouds environment. The implementation shows that the proposed ID-PDP protocol is efficient.

Key words: Cloud storage, Provable Data Possession, Identity-based

⋆ A short version of this paper appeared at ProvSec 2015.

* Corresponding author.
Email address: gaintsky@126.com (Hongyu Liu).