

LETTER

Comparing Performance of Hierarchical Identity-based Signature Schemes

Peixin CHEN^{†a)}, *Member*, Yilun WU[†], Jinshu SU^{†*}, and Xiaofeng WANG[†], *Nonmembers*

SUMMARY Identity-based Signature Scheme is . In this paper,

key words: *Identity-based Signature,*

1. Introduction

2. Preliminaries

2.1 Generic Construction

3. Schemes

3.1 SHER-IBS

3.2 CWS-EF-HIBS

3.3 CWS-HIBOOS

3.4 CWS-EF-HIBOOS

4. Performance Evaluation

In this section, we evaluate the performance of

4.1 Signing/Verification Delay

4.2 Transmission Overhead

5. Conclusions

References

[1]

Manuscript received January 1, 2011.

Manuscript revised January 1, 2011.

[†]The author is with the College of Computer, National University of Defense Technology, Changsha, 410073, China

^{*}The author is with the National Key Laboratory for Parallel and Distributed Processing, National University of Defense Technology, Changsha, 410073, China

a) E-mail: chenpeixin@nudt.edu.cn

DOI: 10.1587/trans.E0.??.