Abstract

We present an ID-based escrow-able authenticated group key agreement (AGKA) protocol which is provably secure in random oracle model. Additionally, the proposed protocol neither involve NAXOS trick nor uses gap assumption. And the security is proven in stronger eCK model. To our best knowledge, the proposed protocol will be first provable Secure and escrow-able ID based authenticated group key agreement protocol without NAXOS trick in eCK model.

References

3. M. Bellare, D. Pointcheval, P. Rogaway, Authenticated key exchange secure against
139155.
6. P. Barreto, H. Kim, B. Lynn, M. Scott, Efficient algorithms for pairing-based
354368.
7. D. Boneh and M. Franklin, Identity-based encryption from the weil pairing, SIAM Journal
8. R. Canetti, H. Krawczyk, Analysis of key-exchange protocols and their use for building
453474.
9. L. Chen, Z. Cheng, and N. P. Smart, Identity-based key agreement protocols from
of the ACM Symposium on Applied Computing, Newfoundland, 2002. 310324
12. Gorantla M C, Boyd C, Nieto J M G. Modeling key compromise impersonation attacks on
group key exchange protocols. In: Proceedings of 12th International Conference on Practice
13. Huang H, Cao Z. An ID-based authenticated key exchange protocol based on bilinear
Inf Theory, 1982, 28: 714720
16. B.A. LaMacchia, K. Lauter, A. Mityagin, Stronger security of authenticated key
18. N. McCullagh, P.S.L.M. Barreto, A new two-party identity-based authenticated key
19. Moriyama D, Okamoto T. An eCK-secure authenticated key exchange protocol without
154167.
104118.
21. Ruxandra F O. Provable secure constant-round group key agreement protocol based on
secret sharing. In: Proceedings of International Joint Conference SOCO13-CISIS13-
ICEUTE13, Salamanca, 2013. 489498.
22. Ustaoglu B. Comparing session state reveal and ephemeral key reveal for Diffie-


Index Terms

Computer Science\hspace{2cm} Security

Keywords

Group key agreement, identity based, escrow-able, NAXOS trick