Cryptology ePrint Archive: Report 2011/225

A Simple and Efficient New Group Key Management Approach Based on Linear Geometry

Shaohua Tang and Jintai Ding and Yujun Liang

Abstract: A new fundamental and secure group key management approach with a group controller GC using the theory of polynomial functions over a vector space over finite field is developed, where each member in the group corresponds to a vector in the vector space and the GC computes a central vector, whose inner product with every member's ID vector are identical. The central vector is published and each member can compute a common group key via inner product. The security relies on the fact that any illegitimate user cannot calculate this value without the legitimate vector, therefore cannot derive the group key. This approach is secure and its backward and forward secrecy can be guaranteed. The performance of our approach is analyzed to demonstrate its advantages in comparison with others, which include: 1) it requires both small memory and little computations for each group member; 2)it can handle massive membership change efficiently with only two re-keying messages, i.e., the central vector and a random number; 3) it is very efficient and very scalable for large size groups. Our experiments confirm these advantages and the implementation of our prototype presents very satisfactory performance for large size groups.

Category / Keywords:

Date: received 8 May 2011

Contact author: shtang at IEEE org

Available formats: PDF | BibTeX Citation

Version: 20110511:121526 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]