東 海 大 學
應 用 數 學 研 究 所
碩 士 論 文

動態會議鑰匙分配系統
Dynamic Conference Key Distribution System

指 導 教 授：沈 淵 源

研 究 生：詹 于 德

中 華 民 國 九 十 六 年 六 月

動態會議鑰匙分配系統
Dynamic Conference Key Distribution System

指導教授:沈淵源　　Advisor:Yuan-Yuan Shen

研 究 生:詹于德　　Student:Yu-Te Chan

東　海　大　學
應　用　數　學　研　究　所
碩　士　論　文

A Thesis Submitted to
Department of Mathematics,College of Science
Tunghai University
in
Partial Fulfillment of the Requirements
for
the Degree of Master of Science
in
Applied Mathematics
June 2007
Taichung,Taiwan,Repulic of China.

中　華　民　國　九　十　六　年　六　月

誌謝

本篇論文得以順利地完成，首先要感謝我的指導教授沈淵源老師，對我的關心與指導。在我最徬徨無助時，抽空指導我，也給我最正確的學習方向，在此表達我的感謝。並且也感謝方源老師及王道明老師給予的意見與指正。

此外，我也得感謝研究所一起陪伴我求學的同學們，謝謝你們的鼓勵與關懷，讓我一路走來，雖又艱辛，但所結的果實是甜美的。

最後，我要感謝我的家人，因爲有他們當我的後盾，讓我在求學的過程中，能毫無後顧之憂，順利完成研究所學業。因此，今後希望能在數學的領域裡能貢獻更多的心力以回饋大家。

詹于德　　謹識於
東海大學應用數學研究所
民國九十六年六月

摘要

本論文主要在探討動態會議鑰匙分配系統。首先，我們先對密碼學做簡單介紹，接著說明相關的背景知識，包括秘密分享、動態秘密分享和橢圓曲線，再應用會議鑰匙分配系統，最後，我們推出一個動態會議鑰匙分配系統並和之前的系統作一簡單的分析。

Abstract

In this thesis, we propose a Dynamic Conference Key Distribution System. We give a very brief introduction to the history of cryptography first, and then discuss its background, including secret sharing,dynamic secret sharing,and ellipitic curve. Next, we use a Conference Key Distribution System. Finally, we present a Dynamic Conference Key Distribution System and make an analysis between this one and the original one.