Abstract

Linear cryptanalysis is one of the most important attacks of block cipher systems such as Feistel netowrks and substitution-permutation networks. In this thesis , we will focus on linear cryptanalysis on SPNs, and give a complete linear attacks on a 4-round SPN with 16-bit block size and 32-bit key length. We will discuss the strategies of linear cryptanalysis on SPNs and give the detial algorithms. We first define the linear probability of an s-box, and use Piling-up Lemma to compute the linear probability of a trail. Then we describe how to find the best trail and then attack the subkey bits. We also study some techniques to improve the success rate of the attack.

Next we give the algorithms of finding the trails, attack strategies, and the backtracking strategy. We will discuss how many plaintext/ciphertext pairs do we need for the given trail. Then we attack a simple SPN structure to show the performance of these strategies.

摘要

線性攻擊法是針對區塊加密系統的最重要的法法之一。在這篇論文裡，我們著重在使用線性攻擊法來攻擊替換排列網路，並且實際的攻擊一個區塊大小為 16 ，金鑰長度為 32 的一個 4 層的替換排列網路。我們將會討論一些在替換排列網路上的線性攻擊法的策略，並給出詳細的演算法。首先我們先了解 s-box 的定義，接著利用 Piling-up Lemma 來計算一條路徑的線性機率的大小。然後我們會說明如何去尋找一條最佳路徑並去攻擊它來求得金鑰的部份內容。我們也會研究一些能夠增加攻擊的成功率的技巧。

之後我們會提出尋找路徑的演算法，攻擊的策略，以及 backtracking 的策略。對於找出來的條路徑，我們會計算我們需要多少組的明文/密文對來做攻擊。最後我們會真正的去攻擊一個替換排列網路，並秀出我們使用這些策略之後的呈現出來的效能。

誌謝

這篇論文的完成，要感謝許多人幫忙：首先要感謝我的指導老師陳榮傑教授，感謝老師兩年來的指導，並在論文研究的過程中，提出了許多的研究方向以及寶貴的意見供我參考，使論文順利完成。其次要感謝我的口試委員曾文貴教授和張仁俊學長，在口試的過程中提出了珍貴的意見，以及糾正我的錯誤，使我的論文能夠更加的完善。

此外也要感謝實驗室的學長們：胡鈞祥學長，黃凱群學長，林賢學長，吳緯凱學長，鄭文鼐學長，感謝他們的幫忙及指導。也感謝和我一起奮鬥的同伴和學弟們，梁漢璋，蔡志彬，劉韋廷，楊葉薰。在這裡也要謝謝交大竹韻口琴社的朋友們，以及 Final Fantasy XI 裡的同伴們，謝謝他們為我加油打氣。

最後要感謝我的父母，感謝他們這六年來辛苦的付出，讓我能夠順利畢業，謝謝你們。