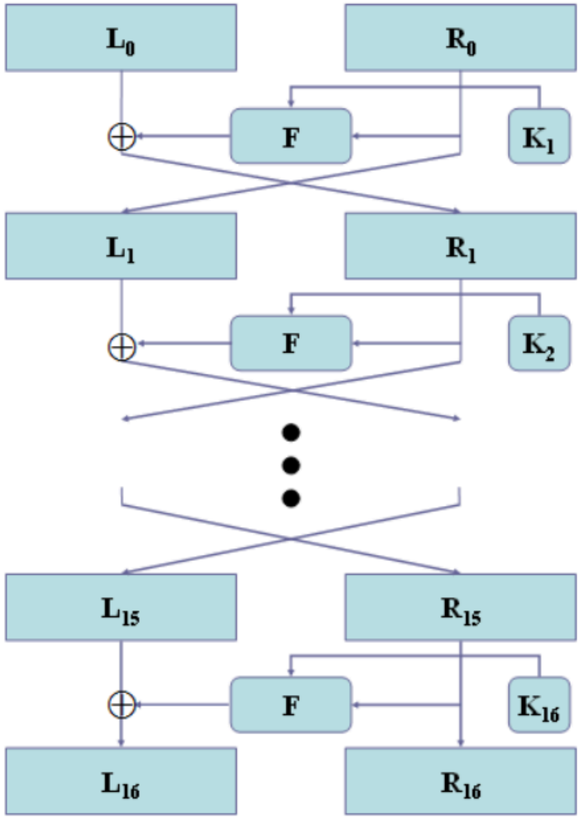
SEED Problem

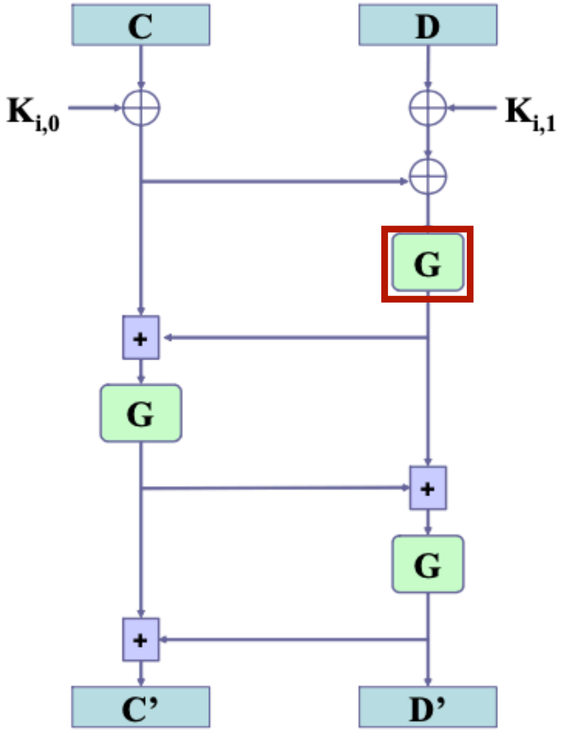
Find master key by CPA

2019330017 백승윤

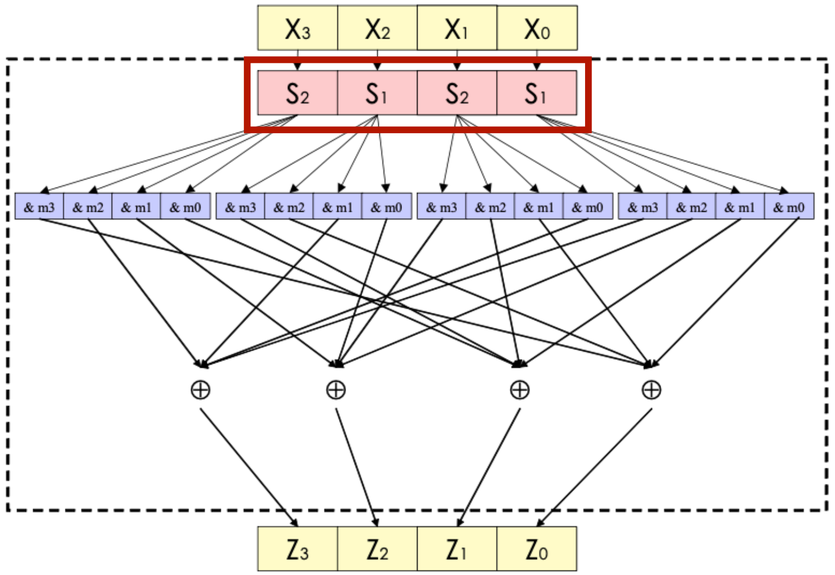
분석 방법



(그림 1) SEED 전체 구조도



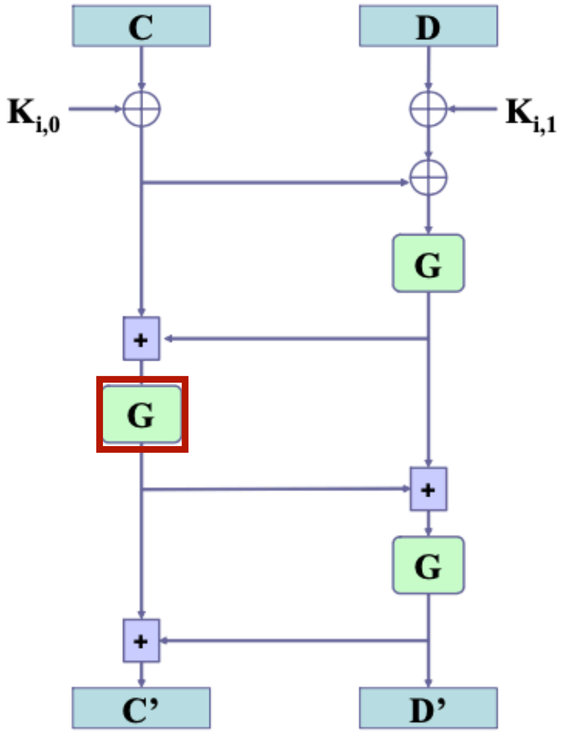
(그림 2) F-함수 구조도



(그림 3) G 함수

$K_{1,0} \oplus K_{1,1}$

분석 방법



(그림 2) F-함수 구조도

Solve $K_{1,0} \rightarrow K_{1,1}$

동일하게 2nd Round Key 계산

Master Key 찾기