2018 암호분석경진대회 : 2번 문제 답안

키 복구 방법이 존재하는 최대 라운드 수 : 12 Round

공격 방법 : 차분 공격을 이용해 12Round Key를 복구한 후 전수조사를 통해 Master Key를 복구한다.

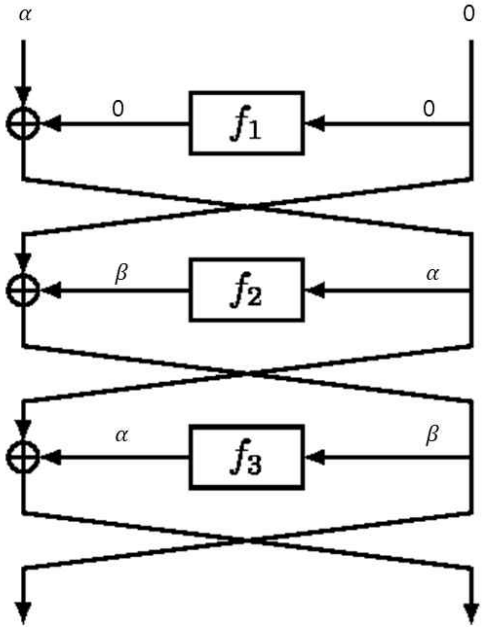
먼저 차분 공격을 하기 위해 차분 테이블을 구한다.

C1 ⊕ C2

P1 ⊕ P2	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	16															
0001				2		2	2	2				2	2		4	
0010										2	2		4	2	2	4
0011		2	2	2				2		4		2	2			
0100										4	4			4	4	
0101			2		4	2			2		2	2			2	
0110		2	2	4		2	2	4								
0111			2		4	2			2	2		2		2		
1000				2		2	2	2				2	2	4		
1001		2	2			2	2			2	2			2	2	
1010		2	2	2				2			4	2	2			
1011		2	2			2	2						4			4
1100		2			4		2		2	2		2		2		
1101				4				4	4							4
1110		2			4		2		2		2	2			2	
1111		2	2			2	2		4							4

2018 암호분석경진대회 : 2번 문제 답안

차분 테이블을 참고하여 반복적인 차분특성을 찾는 것이 첫 번째 목표이다.



차분 관점에서는 Round Key와의 Xor 연산은 영향을 주지 못하므로 라운드함수를 S박스와 P박스로만 생각할 수 있다. 위의 성질을 만족하는 차분을 찾는 방법은 다음과 같다.

첫 번째 시나리오 (없음)

먼저, 입력차분으로 사용할 α의 블록 별 비트 수를 정한다.

입력차분 α가 2Round를 지난 후 다시 α가 나오는 경우를 찾고 있으므로 위의 그림에서 출력차분 또한 α이다.

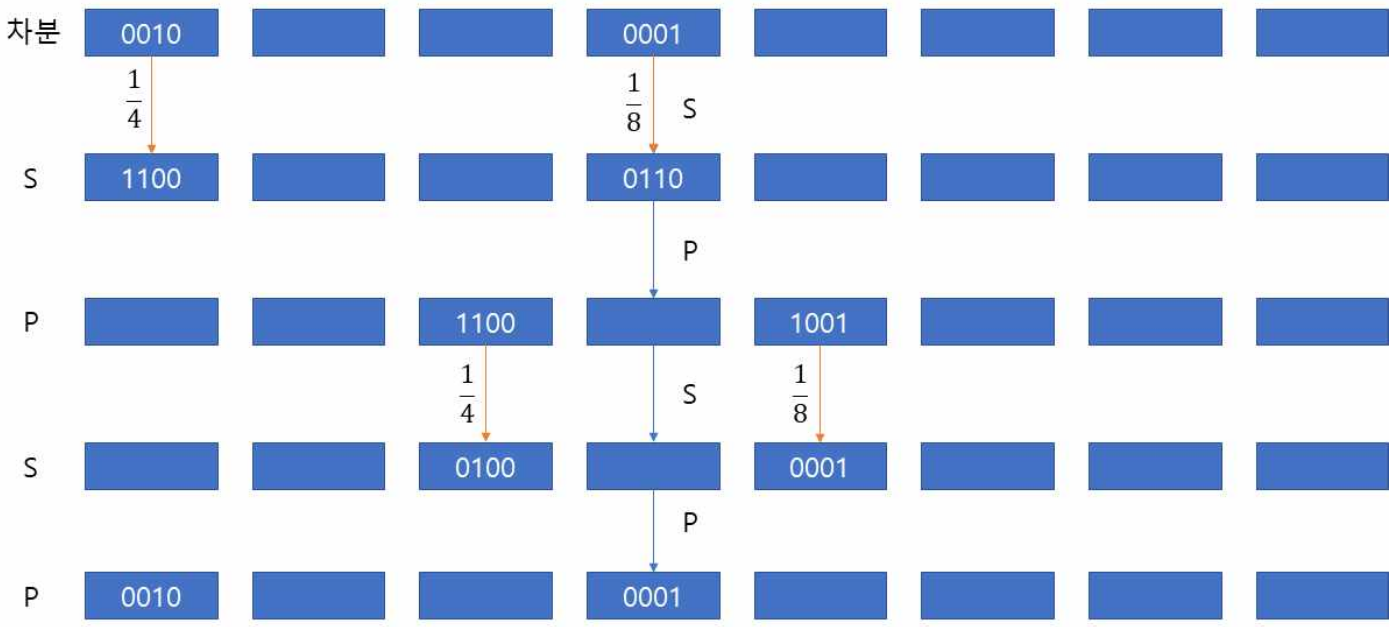
2018 암호분석경진대회 : 2번 문제 답안

다음으로 α가 4비트이므로 $P_2^{-1}(\alpha)$ 또한 4비트여야 함을 알 수 있다. 만약, $P_2^{-1}(\alpha)$가 [0,1,1,0,1,1,0,0]와 같이 1비트씩 4블럭에 확산되어있다면, 0이 아닌 차분을 갖는 S_2-Box는 4개임을 알 수 있다. 이런 경우 $\Pr[f:\beta\rightarrow\alpha \mid f:\alpha\rightarrow\beta]$은 0이 아닌 차분을 갖는 S_2-Box가 2개인 경우보다 일반적으로 낮음을 알 수 있다. 따라서 더 높은 Round에 대해 공격을 하기 위해서 '0'차분을 지닌 S-box가 많이 존재하도록 만드는 것이 특성의 확률을 상대적으로 높게 만들 수 있다.

위의 그림에서처럼 $P_2^{-1}(\alpha)$가 2비트씩 두 블럭에 확산되도록 하는 α를 모두 찾는다. 우리는 α와 $P_2^{-1}(\alpha)$의 몇 번 블록이 0이 아닌 차분을 갖는지 알고 있으므로, $S_1(\alpha)$의 값 또한 몇 번 블록이 0이 아닌 차분을 갖는지 알 수 있다. 따라서 $P_1(S_1(\alpha))$의 값이 $P_2^{-1}(\alpha)$와 같은 블록을 가질 수 있는지 확인한다.

위의 두 가지 조건에 부합하는 α에 대해서 가능한 모든 S-box 근사표를 대입하여 우리가 원하는 차분 쌍을 찾는다. 만약, 찾고자하는 차분 쌍이 존재하지 않을 경우, α의 총 비트 수 및 active S box를 바꿔가며 시행한다.

위와 같은 방법을 통해 입력 차분 α의 비트를 바꿔가며 찾은 차분 쌍은 다음과 같다.



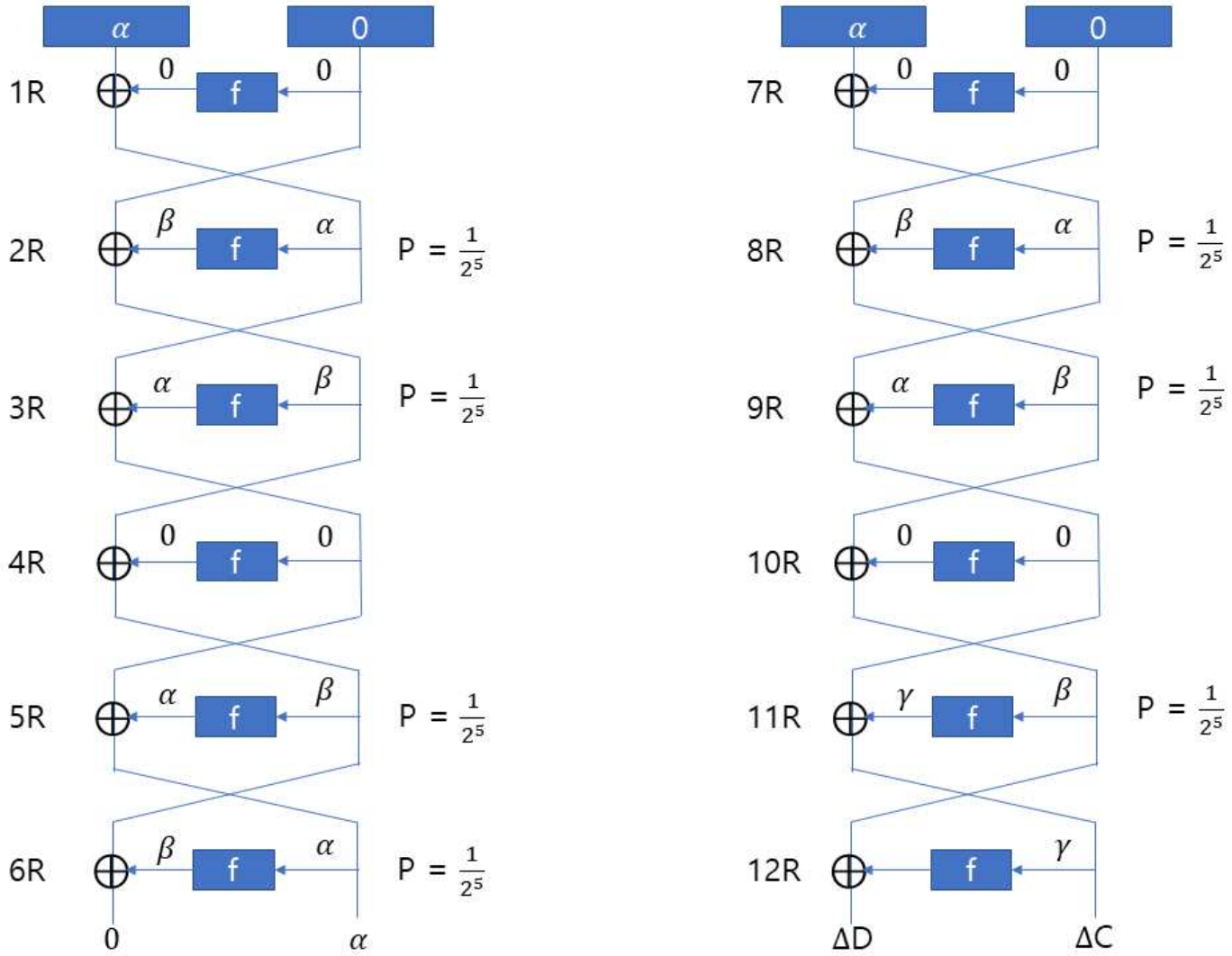
앞으로 α:=0x20010000, β:=0x00c09000 이라고 하면 확률은 다음과 같다.

$$\Pr[f:\alpha\rightarrow\beta]=\frac{1}{2^5}$$

$$\Pr[f:\beta\rightarrow\alpha]=\frac{1}{2^5}$$

공격에 사용할 차분 특성을 그림으로 나타내면 다음과 같다.

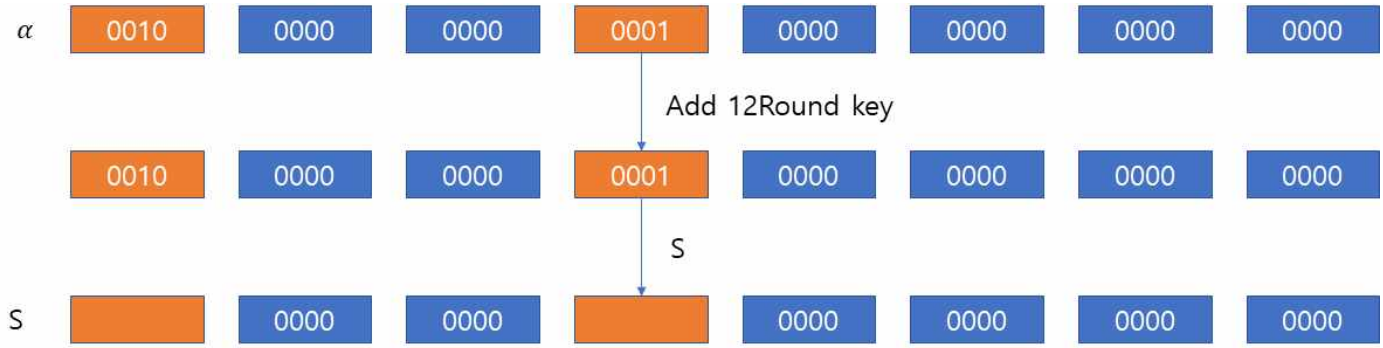
2018 암호분석경진대회 : 2번 문제 답안



우리는 12Round Key를 복구하는 것이 목적이므로 11Round 차분특성을 사용하여 공격한다. 그림에서 보듯이 11Round 특성 확률은 2^{-35}이다. 마지막으로 11Round의 출력차분 $\gamma \in$ {0x04040184, 0x05040184 }라고 정의하자. (31비트는 고정되어있고, 1비트는 free variable로 둔다.)

2018 암호분석경진대회 : 2번 문제 답안

11Round의 입력차분 β에 대해서 출력차분 α을 사용하지 않고 γ를 새로 정의한 이유는 다음과 같다.
만약 11Round의 출력차분을 α로 뒀을 경우,



α=0x20010000이며, active S box는 두 개뿐이므로 12Round key를 찾을 때 active S box에 해당하는 8비트만 찾을 수 있다. 따라서 차분 특성을 만족시킬 확률이 동일하다면, 11Round에는 더 많은 active S box를 갖는 차분특성을 이용하는 것이 효율적이다.
위에 정의한 γ에 대해서는 active S box가 5개이므로 12Round key 20비트를 구할 수 있다.

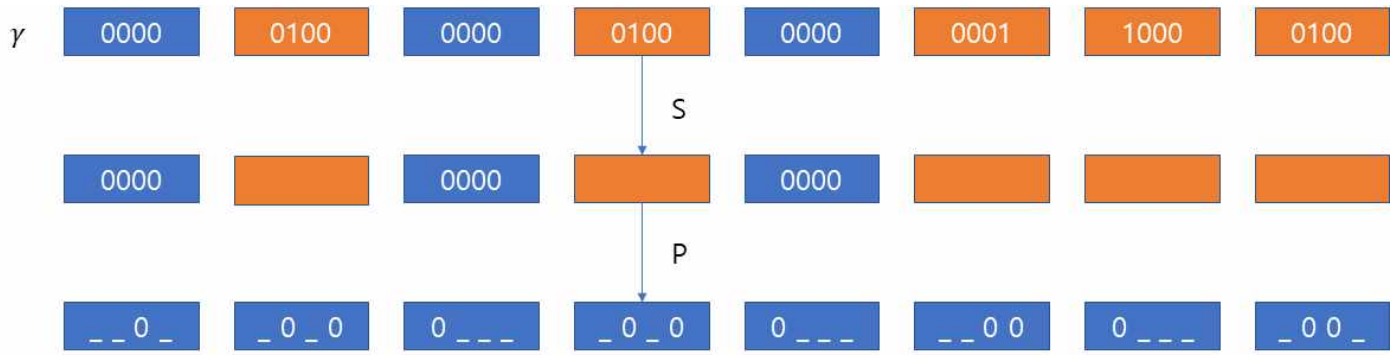
공격하는 방법은 다음과 같다.

1. 2^{38}개의 입력차분 (α,0)에 대한 12Round 암호문을 오라클로부터 획득한다.
2. 2^{38}개의 암호문 차분 쌍에 대해서 12Round의 키를 추측하여 부분복호화를 진행한다. 키를 추측할 때, acitve S box가 5개이므로 S box의 영향을 받는 20bit를 제외한 나머지 bit는 0으로 놓고 20비트에 대한 전수조사만을 진행한다.
3. 12Round 부분 복호화한 값들에 대해서 차분을 계산한 결과가 (γ, β)인 경우 복호화에 사용된 key에 대한 count 값을 1 증가시킨다. 여기서 count가 가장 높은 key가 Right key의 후보가 된다.

하지만 여기서, 2^{39}개의 암호문을 전부 부분복호화 할 필요는 없다. 만약, 암호문 차분쌍 $\triangle C$가 γ가 아니라면, 12Round를 부분 복호화했을 때의 차분이 (γ, β)될 수가 없으므로 Wrong Pair라고 할 수 있다.

2018 암호분석경진대회 : 2번 문제 답안

γ = 0x04040184 또는 0x05040184이므로 $\triangle C$ = γ인 암호문 차분쌍에 대해서만 부분복호화를 진행하면 많은 Wrong Pairs를 제거할 수 있다. 뿐만 아니라, $\triangle D$에서도 Wrong Pairs를 제거할 수 있다.



γ는 active S-box가 5개이므로 3개의 S-box에는 0차분이 대응되며 그 결과, 위와 같이 12비트는 0으로 고정되어야 한다는 사실을 알 수 있다.

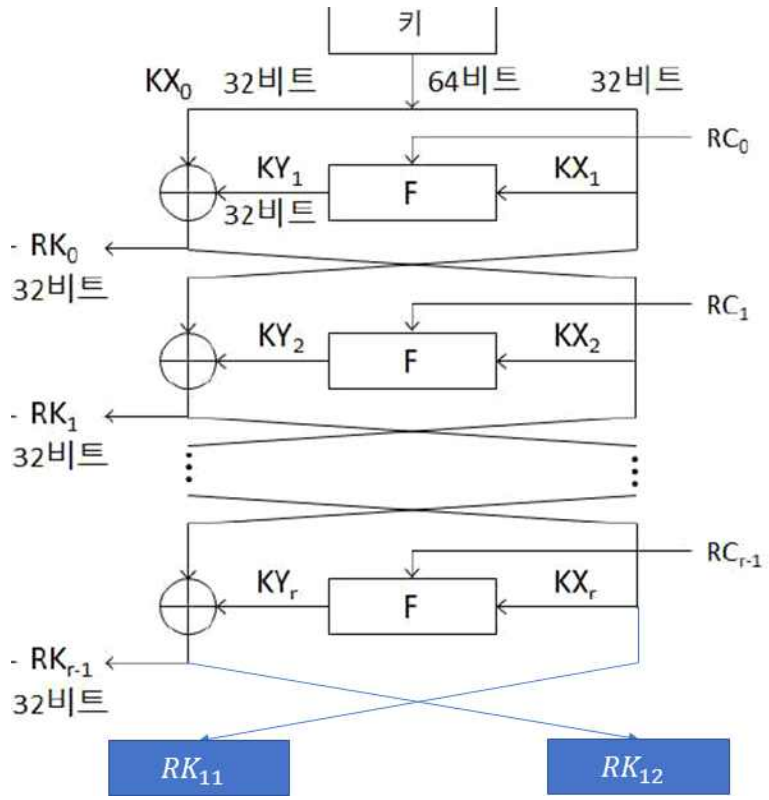
2^{38}개의 입력차분 $(\alpha,0)$에 대한 출력차분을 위와 같은 필터링을 거치면, 11Round 특성확률이 2^{-35}이고 Wrong Pairs는 2^{-43}($\triangle C$가 γ이므로 31비트 고정이며 $\triangle D$에서 12비트가 0으로 고정이기 때문)으로 상대적으로 작기 때문에, 위의 조건을 만족하는 암호문 차분은 약 $2^{38}*(2^{-35}+2^{-44})$ = 2^{3} 정도가 된다. 즉, Right Pairs일 확률이 Wrong Pairs 보다 훨씬 크므로, 대부분이 Right Pairs 라고 할 수 있다.

따라서 12Round key 20bit에 대한 전수조사의 시간 복잡도는 약 $O(2^4*2^{20}*\frac{1}{12})=O(2^{21})$정도 된다.

* 2^4 : 암호문의 개수
* 2^{20} : 12Round key 20비트 전수조사 횟수
* $\frac{1}{12}$: 1Round 복호화 시간 복잡도 (12Round 암호화 시간 복잡도 = 1)

2018 암호분석경진대회 : 2번 문제 답안

Master key를 복구하는 방법은 다음과 같다.



위의 그림에서 우리는 RK_{12}의 20bits를 알고 있는 상황이며, RK_{11}의 값은 전혀 모르는 상태이다. 하지만, RK_{11}, RK_{12}의 값을 모두 안다면 (RC값이 공개되어 있으므로), 복호화 과정을 진행하여 마스터키인 KX_0, KX_1의 값을 찾을 수 있다. 따라서 RK_{11}(32bits)와 RK_{12}(12bits)에 대해서 전수조사를 진행한다.

RK_{11}와 RK_{12}을 전수 조사하는 과정에서 만들어진 마스터키가 적합한지 확인하기 위해서 이전에 오라클에 질의했던 (평문, 암호문) 쌍을 이용한다. 즉, 만들어진 마스터키를 가지고 평문을 암호화한 값이 오라클에 질의했던 암호문과 일치하는 지를 비교하여 일치하지 않는 경우, 새로운 마스터키를 생성한다.

이 때, 필요한 평균 시간 복잡도는 $O(2^{44})$이다. 마스터키를 추출하는 데에 있어서 걸리는 평균 시간 복잡도는 $O(2^{43})$이지만, 해당 마스터키가 옳은 키인지 검증하는 과정이 필요하므로 평균 시간 복잡도는 $O(2^{44})$가 된다.

따라서,

데이터 복잡도 : $O(2^{39})$

시간 복잡도 : $O(2^{44})$

을 사용하여 12Round 블록암호의 마스터키를 복구할 수 있다.