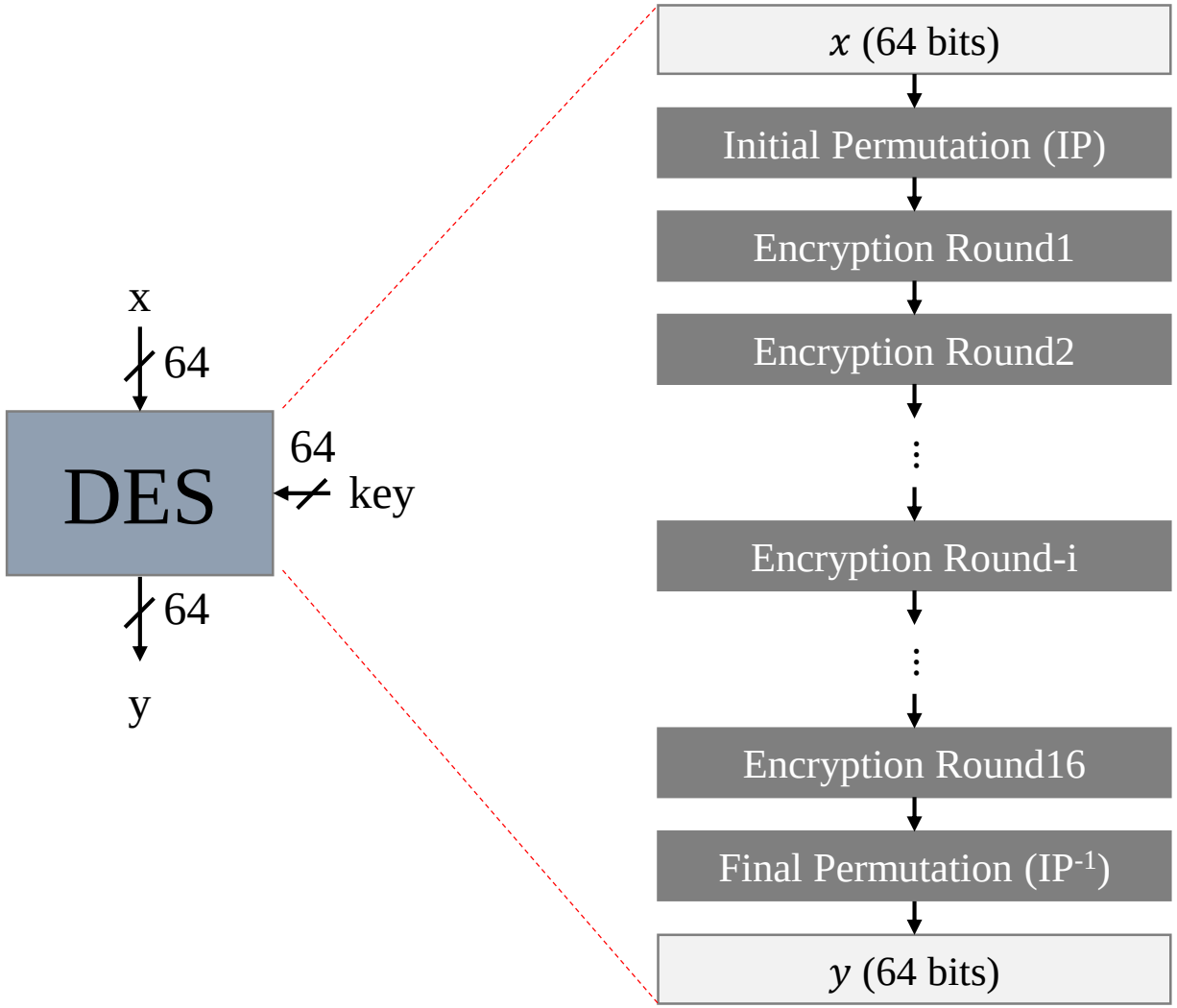
DES

논리회로실습

부경대 컴퓨터공학부 최필주

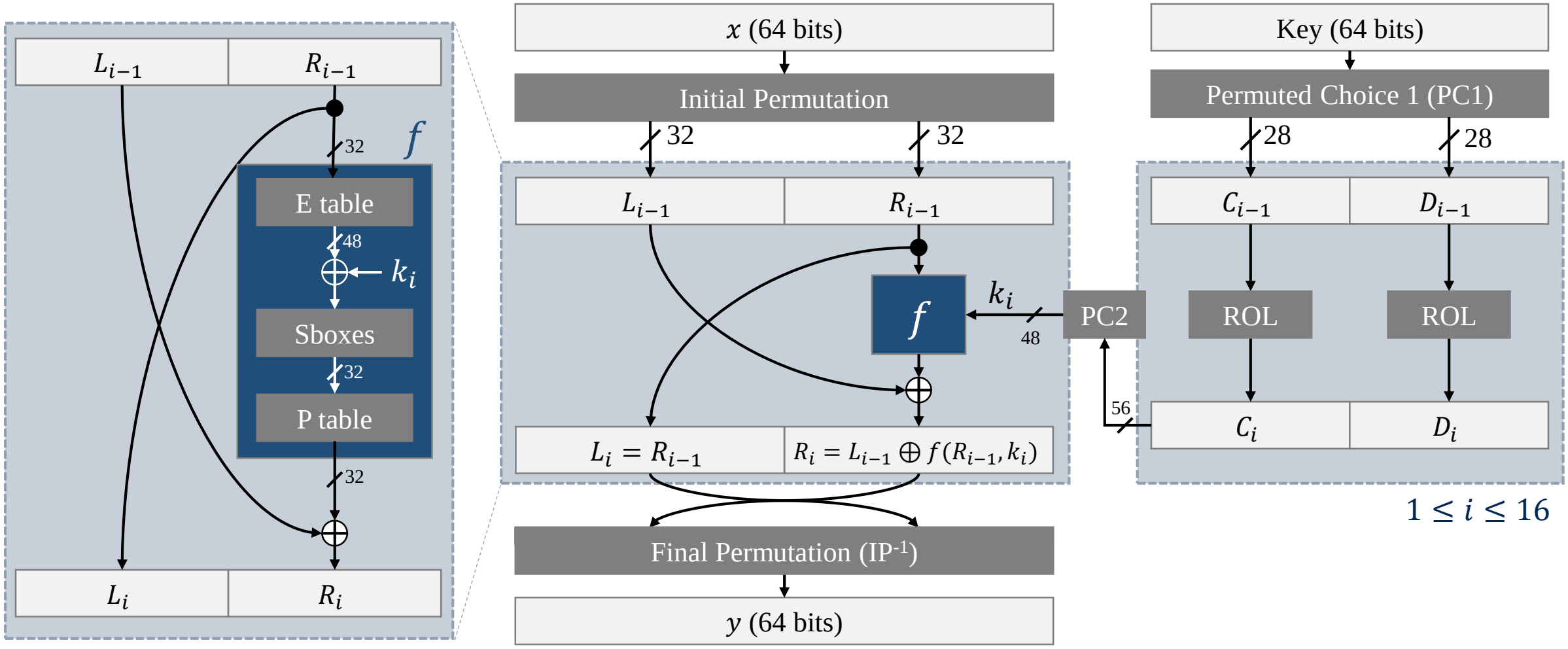
DES 알고리즘

- 알고리즘 개요



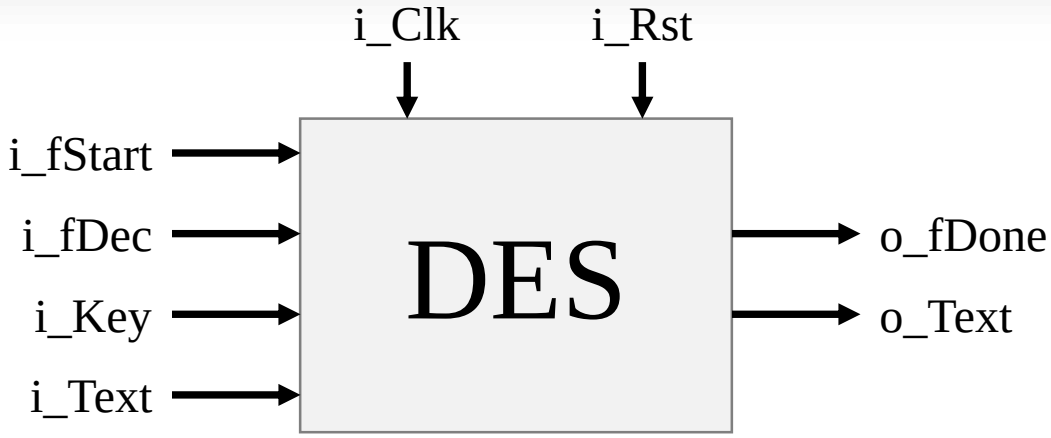
DES 알고리즘

- 알고리즘 상세



하드웨어 설계

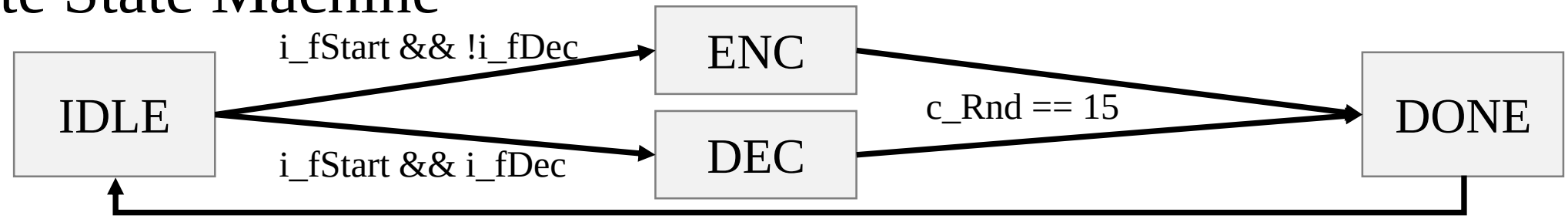
- 입력과 출력



이름	구분		bits	설명
i_Clk	입력	기본	1	positive clock 신호
i_Rst			1	negative reset 신호(0: reset, 1: 동작)
i_fStart		제어	1	DES 동작 신호
i_fDec			1	암복호화 선택 신호(0: 암호화, 1: 복호화)
i_Key		데이터	64	key
i_Text			64	입력 text(암호화: plain-text, 복호화: cipher-text)
o_fDone	출력	상태	1	
o_Text		데이터	64	출력 text(암호화: cipher-text, 복호화: plain-text)

하드웨어 설계

- Finite State Machine



		bits	IDLE		ENC	DEC	DONE
			i_fStart = 0	i_fStart = 1			
Regs.	n_Rnd	4	0		c_Rnd + 1		0
	{n_L, n_R}	32+32	0	IP(i_Text)	{c_R, c_L ^ f(c_R, PC2({c_C, c_D}))}		0
	{n_C, n_D}	28+28	0	i_fDec ? PC1(i_Key) : ROL(PC1(i_Key), 1)	{ROL(C, 1 or 2), ROL(D, 1 or 2)}	{ROL(C, -1 or -2), ROL(D, -1 or -2)}	0
Output	o_fDone	1	0		0		1
	o_Text	64	0		0		IP^{-1}({c_R, c_L})

- ROL({C, D}, n): C, D 각각 n-bit left rotation
- f(R, K): P_table $\left(\mathrm{SBOX}\left(\mathrm{E\_table}(R) \oplus \mathrm{PC2}(K)\right)\right)$

하드웨어 설계

- Text vector