Triple-DES 양자회로 구현

https://youtu.be/mcecWs9CvuY

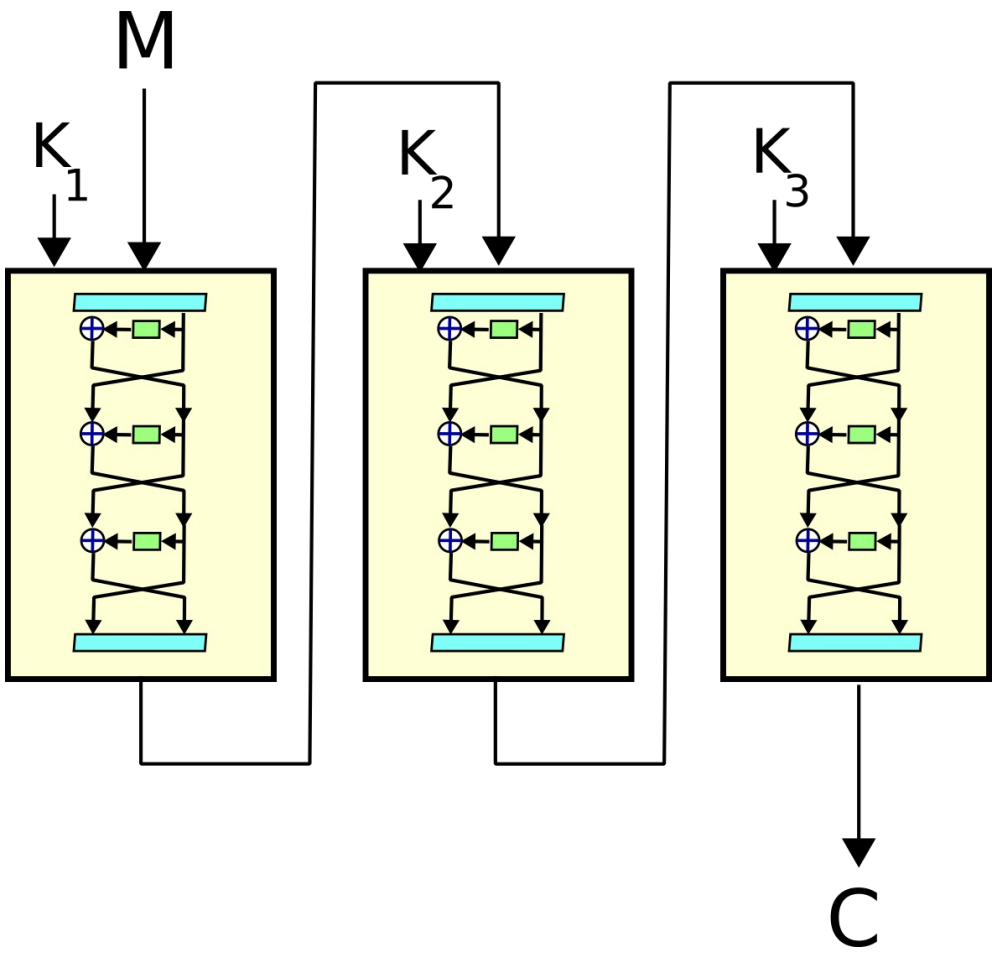
정보컴퓨터공학과 송경주

Triple-DES (TDES)

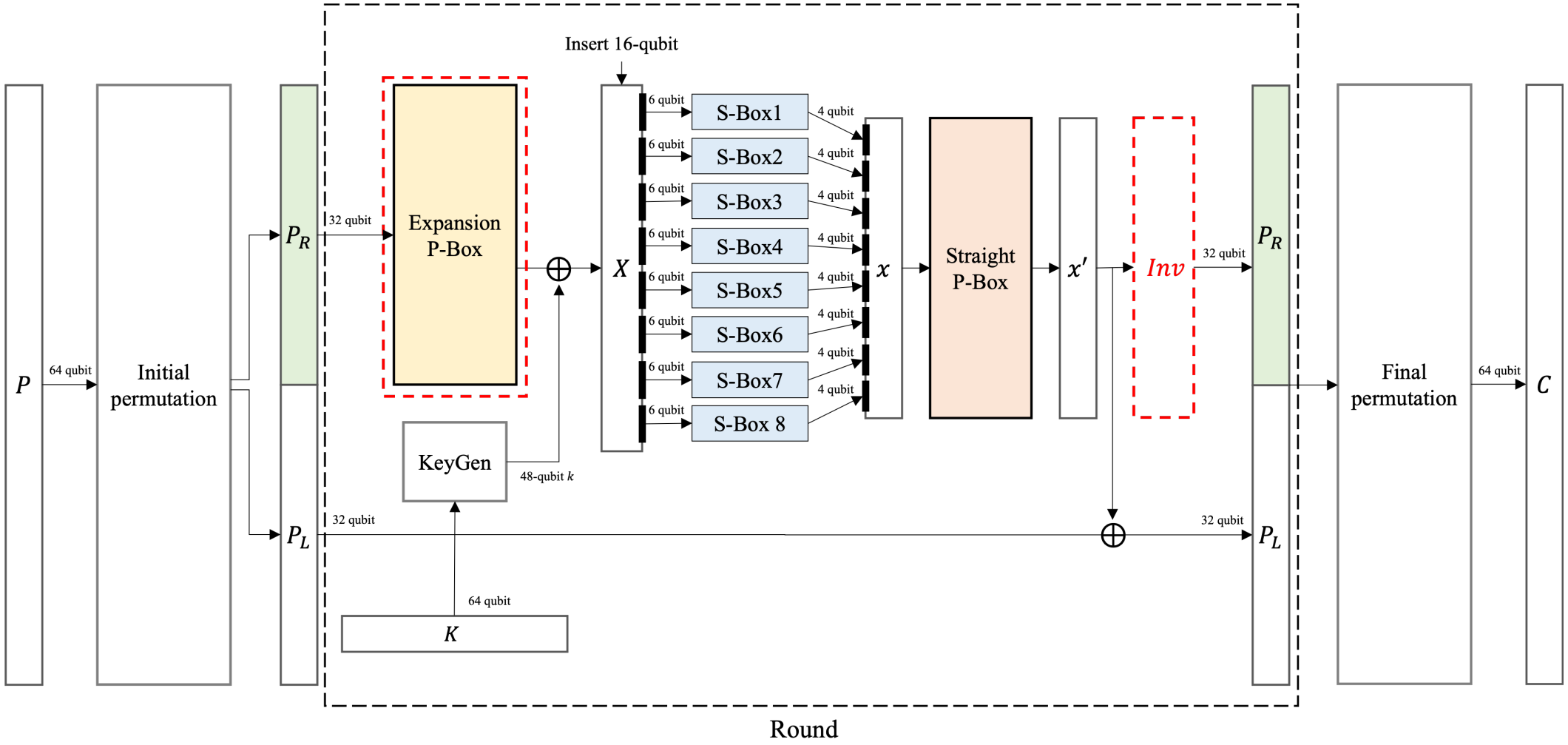
- Triple-DES(TDES): DES의 보안 취약점에 대한 대응으로 개발된 Triple DES는 DES를 연속 3회 적용하여 보안을 강화한 암호화 알고리즘

- 암호화 및 복호화에 각각 168(56*3)비트 키를 사용

- 사용하는 암호키 길이가 커져 DES의 보안 문제를 해결하였지만 속도 측면에서 느림



Triple-DES (TDES) 양자회로



Triple-DES (TDES) 양자회로

- Expansion P-Box
  - 구현 방향에 따라 사용하는 양자자원이 달라짐
  - 세 가지 구현으로 나눠서 결과 비교 진행

<Basic>
- 기존 DES 연산 순서에 따라 진행하는 방식
- 32bit P를 48bit로 확장시켜야 하므로 매 라운드 16-qubit가 추가로 사용됨

(DES: 16*16 = 256 qubit, TDES: 16*16*3 = 768 qubit)

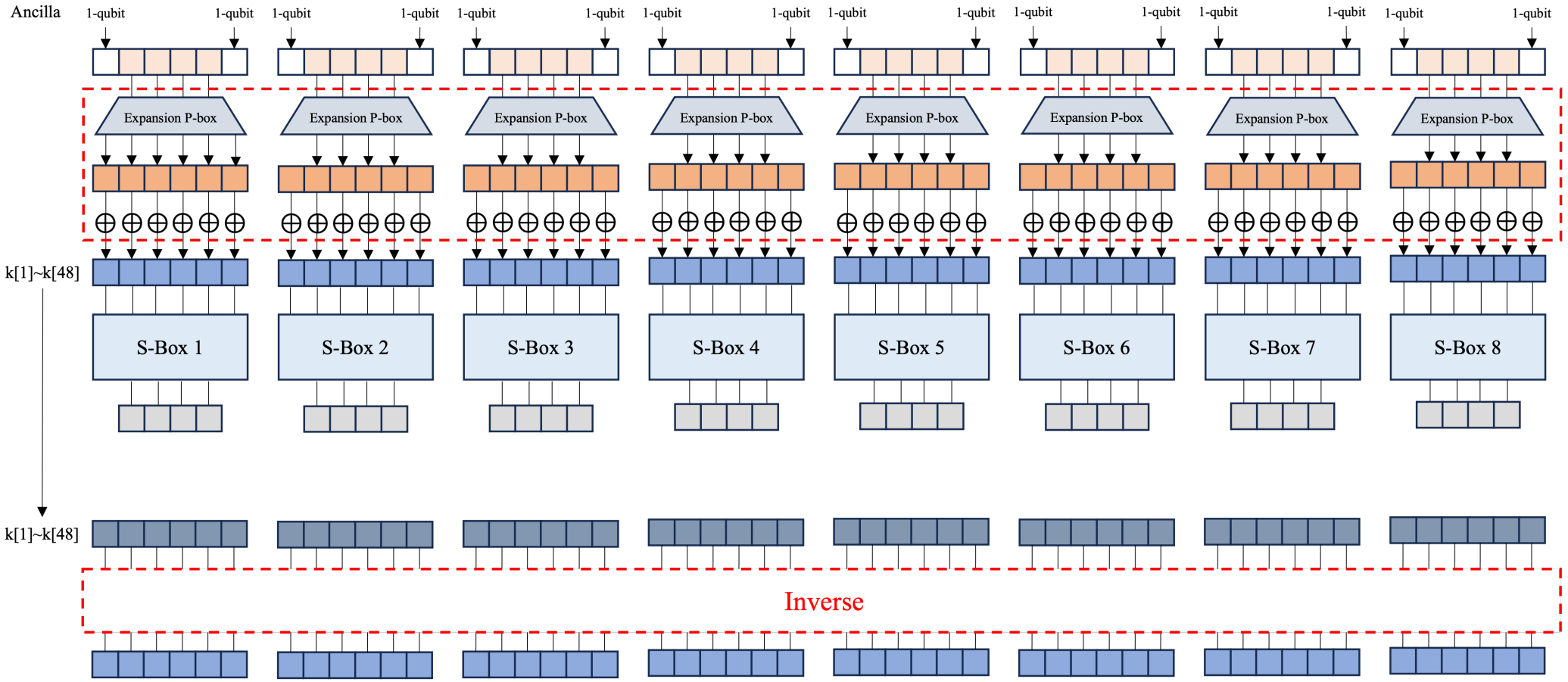
<Type A>
- 기존 DES 연산 순서를 변경하여 큐비트 사용을 줄이는 방식
- 확장된 48-bit와 key의 XOR 결과를 key에 저장하도록 하여 큐비트 할당을 하지 않음 (중복으로 사용되는 48-bit에 대해 확장 전 32-qubit과 일치하는 인덱스와 XOR)
- Key는 다음에 다시 사용해야하므로 key를 inverse하기 위한 연산이 추가됨

<Type B>
- 기존 DES 연산 순서를 변경하여 큐비트 사용을 줄이는 방식
- 48bit로 확장될 32bit P에서 중복으로 사용되는 큐비트를 중복으로 사용함

(사용이 겹치지 않게 S-Box를 배치)
- P를 중복으로 사용하기 위해 한번 사용을 마친 후 다시 inverse하는 연산이 추가됨

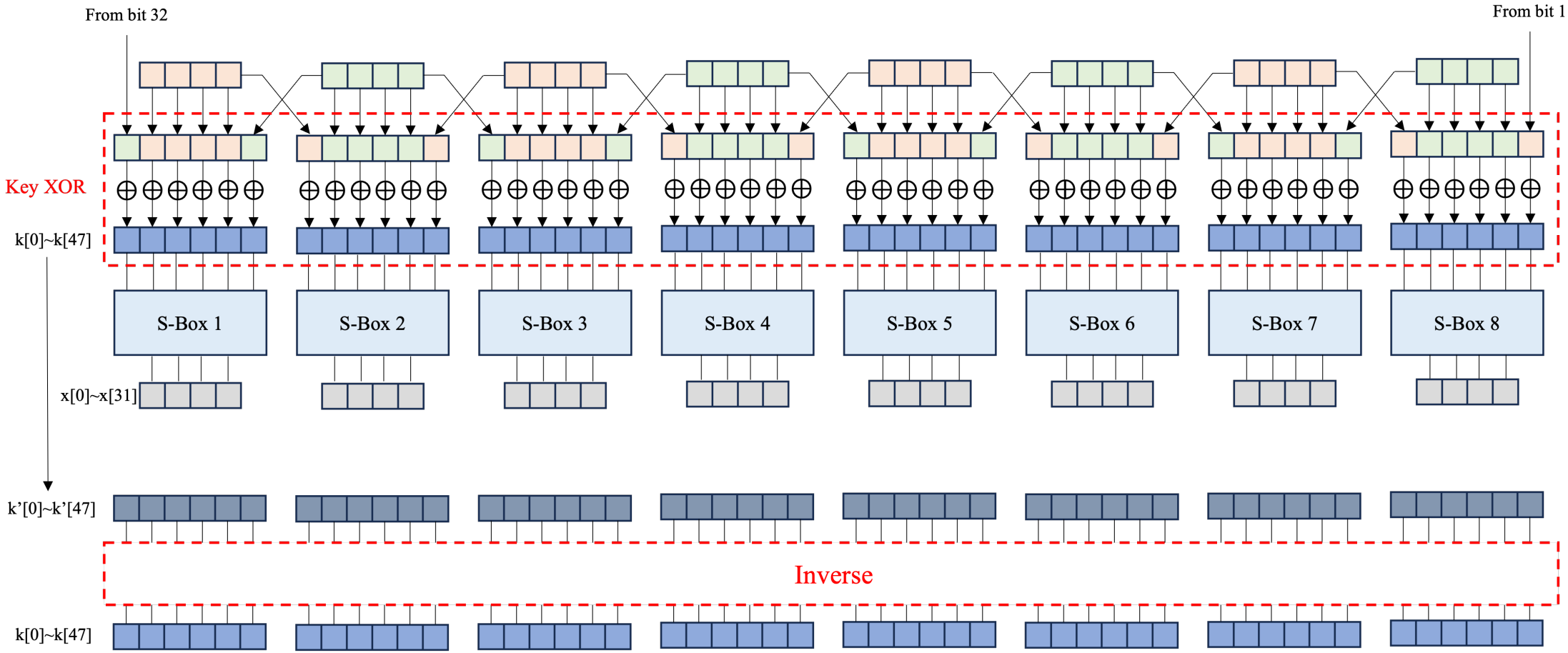
Triple-DES (TDES) 양자회로

- Expansion P-Box : Basic



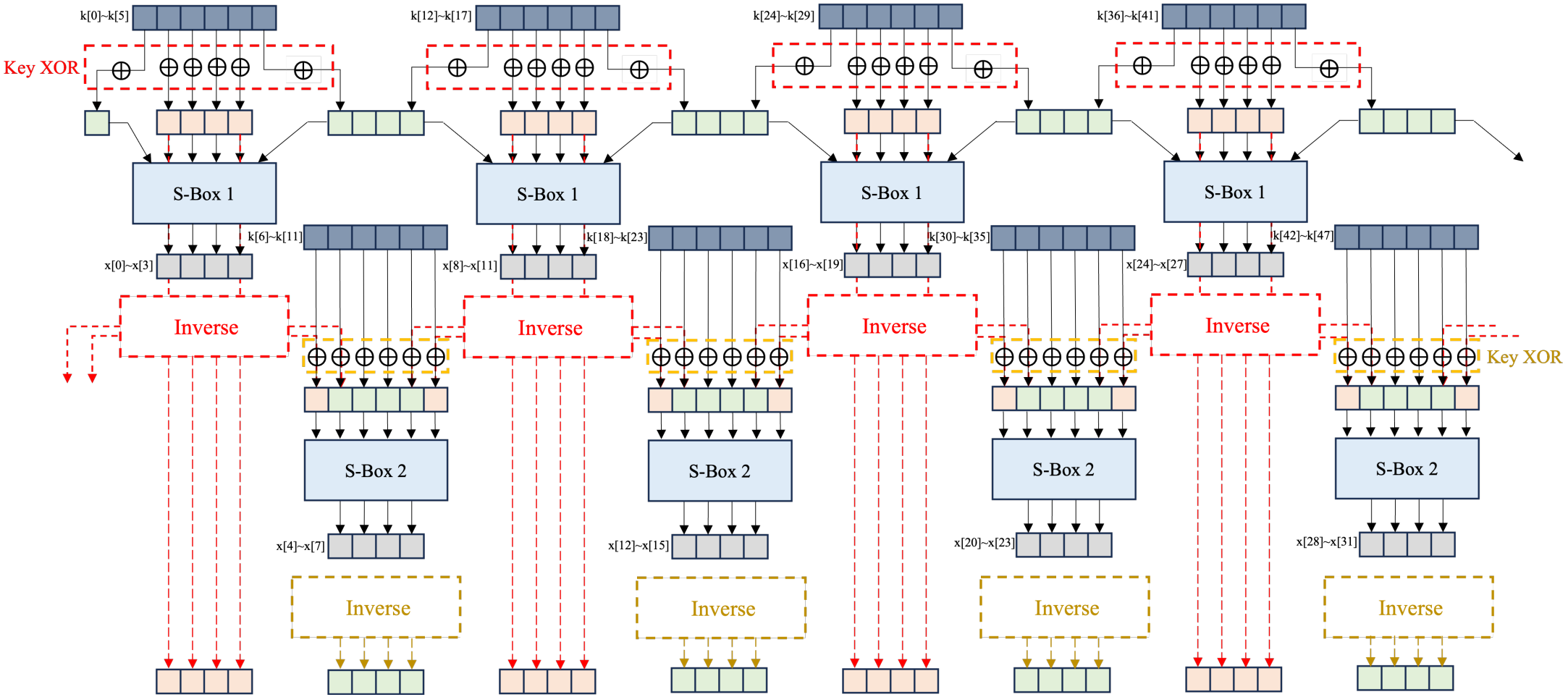
Triple-DES (TDES) 양자회로

- Expansion P-Box : Type A



Triple-DES (TDES) 양자회로

- Expansion P-Box : Type B



Triple-DES (TDES) 양자회로

- Expansion P-Box

Function	Quantum resources				
	Qubit	Toffoli	CNOT	1qClifford	Depth
Basic	816	6,848	20,160	11,232	2,162
Type A	560	6,848	19,648	11,232	2,192
Type B	–	–	–	–	–

Table 1: The estimation results of quantum resources by applying Expansion P-Box Types A and B to qubit-optimized quantum circuit.

Function	Quantum resources				
	Qubit	Toffoli	CNOT	1qClifford	Depth
Basic	7,536	3,424	12,992	7,184	1,044
Type A	7,280	3,424	12,480	7,184	1,044
Type B	7,280	3,424	12,480	7,184	1,661

Table 2: The estimation results of quantum resources by applying Expansion P-Box Types A and B to depth-optimized quantum circuit.

Triple-DES (TDES) 양자회로

- S-Box
  - 구현 방향에 따라 사용하는 양자자원이 달라짐
  - 네 가지 구현으로 나눠서 결과 비교 진행

<Type A>
  - S-Box 내부에서 ancilla 큐비트를 inverse 후 **다음 S-Box**에서 재사용
  - Ancilla 큐비트 중 결과를 저장하는 4-qubit만 재사용 불가, 나머지는 재사용 가능
  - Ancilla 큐비트 N 중 N-4개의 큐비트를 리셋하기 위한 연산이 추가됨
  - S-Box 1~8에서 같은 ancilla 사용 → 병렬 불가능, 사용 가능한 ancilla 큐비트 수 N-(4*(n-1))로 줄어듦 (n: S-Box 순서)

<Type B>
  - S-Box 내부에서 ancilla 큐비트를 inverse 후 **다음 S-Box**에서 재사용 (모두 재사용 가능)
  - 결과를 저장하는 4-qubit를 계속 할당하여 사용
  - Ancilla 큐비트 N을 리셋하기 위한 연산이 추가됨
  - S-Box 1~8에서 같은 ancilla 사용 → 병렬 불가능, 사용 가능한 ancilla 큐비트 유지됨

Triple-DES (TDES) 양자회로

- S-Box

<Type C>

- S-Box 내부에서 ancilla 큐비트를 inverse 후 **다음 라운드**에서 재사용
- 8개의 ancilla 큐비트 중 결과를 저장하는 4-qubit만 재사용 불가, 나머지는 재사용 가능
- 각 8개의 ancilla N 큐비트 중 N-4개의 큐비트를 리셋하기 위한 연산이 추가됨
- S-Box 1~8에서 각각의 ancilla 사용 (8개) → 병렬 가능, 각 S-Box 별 사용 가능한 ancilla 큐비트 수 N-(4*(r-1)) 로 줄어듦 (r: 라운드 수)

<Type D>

- S-Box 내부에서 ancilla 큐비트를 inverse 후 **다음 라운드**에서 재사용 (모두 재사용 가능)
- 결과를 저장하는 4-qubit를 계속 할당하여 사용
- 8개의 ancilla N 큐비트를 리셋하기 위한 연산이 추가됨
- S-Box 1~8에서 각각의 ancilla 사용 (8개) → 병렬 가능, 각 S-Box 별 사용 가능한 ancilla 큐비트 유지됨

Triple-DES (TDES) 양자회로

S-Box	Ancilla		Inverse point	Parallel
	Register	Result		
Type A	One n-qubit	0	S-Box	X
Type B	One n-qubit	$4 \times 8 \times r$	S-Box	X
Type C	Eight $n + @$ qubits	0	Round	O
Type D	Eight n qubits	$4 \times 8 \times r$	Round	O

Table 5: Characteristics of Different Types of S-Boxes.

Triple-DES (TDES) 양자회로

Opt.	P-Box	S-Box	
		Version 1	Version 2
Qubit	Basic	Basic Type A Type B Type C Type D	Basic Type A Type B Type C Type D
	Type A	Basic Type A Type B Type C Type D	Basic Type A Type B Type C Type D
	Type B	- Type A Type B Type C Type D	- Type A Type B Type C Type D
Depth	Basic	Basic Type A Type B Type C Type D	Basic Type A Type B Type C Type D
	Type A	Basic Type A Type B Type C Type D	Basic Type A Type B Type C Type D
	Type B	Basic Type A Type B Type C Type D	Basic Type A Type B Type C Type D

Table 6: Combinations for DES Quantum Circuit

Triple-DES (TDES) 양자회로

Depth optimized DES

S-Box(.ver 1)

Function		Quantum resources				
S-Box	P-Box	Qubit	Toffoli	CNOT	1qClifford	Depth
Basic	Basic	7,536	3,424	12,992	7,184	1,044
	A	7,280	3,424	12,480	7,184	1,044
	B	7,280	3,424	12,480	7,184	1,661
A	Basic	930	6,848	19,328	11,488	12,469
	A	674	6,848	18,816	11,488	12,469
	B	674	6,848	18,816	11,488	12,468
B	Basic	936	7,072	18,368	11,456	14,774
	A	680	7,072	17,856	11,456	14,773
	B	680	7,072	17,856	11,456	14,772
C	Basic	1,296	6,848	19,328	11,488	1,938
	A	1,040	6,848	18,816	11,488	1,968
	B	1,040	6,848	18,816	11,488	2,605
D	Basic	1,288	7,072	18,368	11,456	2,322
	A	1,032	7,072	17,856	11,456	2,352
	B	1,032	7,072	17,856	11,456	2,843

Table 7: Estimation of quantum resources for depth-optimized DES quantum circuits. (S-Box version 1: S-Box composed of standard gates)

가장 적은 큐비트

S-Box(.ver 2)

Function		Quantum resources				
S-Box	P-Box	Qubit	Toffoli	CNOT	1qClifford	Depth
Basic	Basic	6,896	3,536	11,536	7,600	1,012
	A	6,640	3,536	11,024	7,600	1,011
	B	6,640	3,536	11,024	7,600	1,468
A	Basic	926	7072	16,960	11,392	13,750
	A	670	7,072	16,448	11,392	13,749
	B	670	7,072	16,448	11,392	13,748
B	Basic	936	7,072	18,368	11,104	15,078
	A	680	7,072	17,856	11,104	15,077
	B	680	7,072	17,856	11,104	15,076
C	Basic	1,256	7,072	16,960	11,392	1,986
	A	1,000	7,072	16,960	11,392	2,016
	B	1,000	7,072	16,448	11,392	3,405
D	Basic	1,288	7,072	18,368	11,104	2,354
	A	1,032	7,072	17,856	11,104	2,384
	B	1,032	7,072	17,856	11,104	2,907

Table 8: Estimation of quantum resources for depth-optimized DES quantum circuits. (S-Box version 2: S-Box composed of non-standard gates)

가장 작은 Depth

Triple-DES (TDES) 양자회로

Qubit optimized DES

S-Box(.ver 1)

Function		Quantum resources				
S-Box	P-Box	Qubit	Toffoli	CNOT	1qClifford	Depth
Basic	Basic	816	6,848	20,160	11,232	2,162
	A	560	6,848	19,648	11,232	2,192
	B	–	–	–	–	–
A	Basic	930	13,664	35,872	21,760	24,768
	A	674	13,664	35,360	21,760	24,768
	B	674	6,848	18,816	11,488	12,468
B	Basic	936	14,080	33,856	21,888	29,314
	A	680	14,080	33,344	21,888	29,312
	B	680	7,072	17,856	11,456	14,772
C	Basic	1,296	6,848	19,328	11,488	1,938
	A	1,040	6,848	18,816	11,488	1,968
	B	1,040	6,848	18,816	11,488	2,605
D	Basic	1,288	13,444	32,262	18,598	4,322
	A	1,032	13,440	31,744	18,592	4,352
	B	1,032	7,072	17,856	11,456	2,843

Table 9: Estimation of quantum resources for qubit-optimized DES quantum circuits. (S-Box version 1: S-Box composed of standard gates)

가장 작은 Depth

S-Box(.ver 2)

Function		Quantum resources				
S-Box	P-Box	Qubit	Toffoli	CNOT	1qClifford	Depth
Basic	Basic	776	7,072	17,856	11,104	2,354
	A	520	7,072	17,344	11,104	2,384
	B	–	–	–	–	–
A	Basic	926	14,080	31,040	21,792	27,266
	A	670	14,080	30,528	21,792	27,264
	B	670	7,072	16,448	11,392	13,748
B	Basic	1,288	13,412	32,262	20,074	4,386
	A	680	14,080	33,344	21,472	29,888
	B	680	7,072	17,856	11,104	15,076
C	Basic	1,256	7,072	16,960	11,392	1,986
	A	1,000	7,072	16,448	11,392	2,016
	B	1,000	7,072	16,448	11,392	3,405
D	Basic	1,288	13,412	32,262	20,074	4,386
	A	1,032	13,408	31,744	20,064	4,416
	B	1,032	7,072	17,856	11,104	2,907

Table 10: Estimation of quantum resources for qubit-optimized DES quantum circuits. (S-Box version 2: S-Box composed of non-standard gates)

가장 적은 큐비트

Triple-DES (TDES) 양자회로

Function		Quantum resources				
S-Box	P-Box	Qubit	Toffoli	CNOT	1qClifford	Depth
Ver.1 Basic	Basic	22,384	10,272	38,976	21,552	3,124
Ver.2 Type A	Type B	1,694	21,216	49,344	34,176	41,236
Ver.2 Type B	Type A	1,704	21,216	53,568	33,312	45,221
Ver.2 Basic	Type A	19,696	10,608	33,072	22,800	3,027

가장 작은 depth

Table 11: Estimation of quantum resources for TDES (Fow of DES: Depth-optimized)

Function		Quantum resources				
S-Box	P-Box	Qubit	Toffoli	CNOT	1qClifford	Depth
Ver.1 Type C	Basic	2,832	20,544	57,984	34,464	5,810
Ver.2 Basic	Type A	520	21,216	52,032	33,312	7,152
Ver.2 Type B	Type A	1,704	42,240	100,032	64,416	89,664
Ver.1 Type C	Basic	2,832	20,544	57,984	34,464	5,810

가장 적은 큐비트

Table 12: Estimation of quantum resources for TDES (Fow of DES: Qubit-optimized)

Q & A