TDES 양자 보안 강도 평가

https://youtu.be/xEmgKqtonnc

정보컴퓨터공학과 송경주

DES 양자회로

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

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

S-Box

S-Box	Ancilla qubit		Inverse point	Parallel
	Register	Result		
Type A	n-qubit	$4 \times 8 \times r$	S-Box	X
Type B	$8n$ qubits	$4 \times 8 \times r$	Round	O

Expansion P-Box

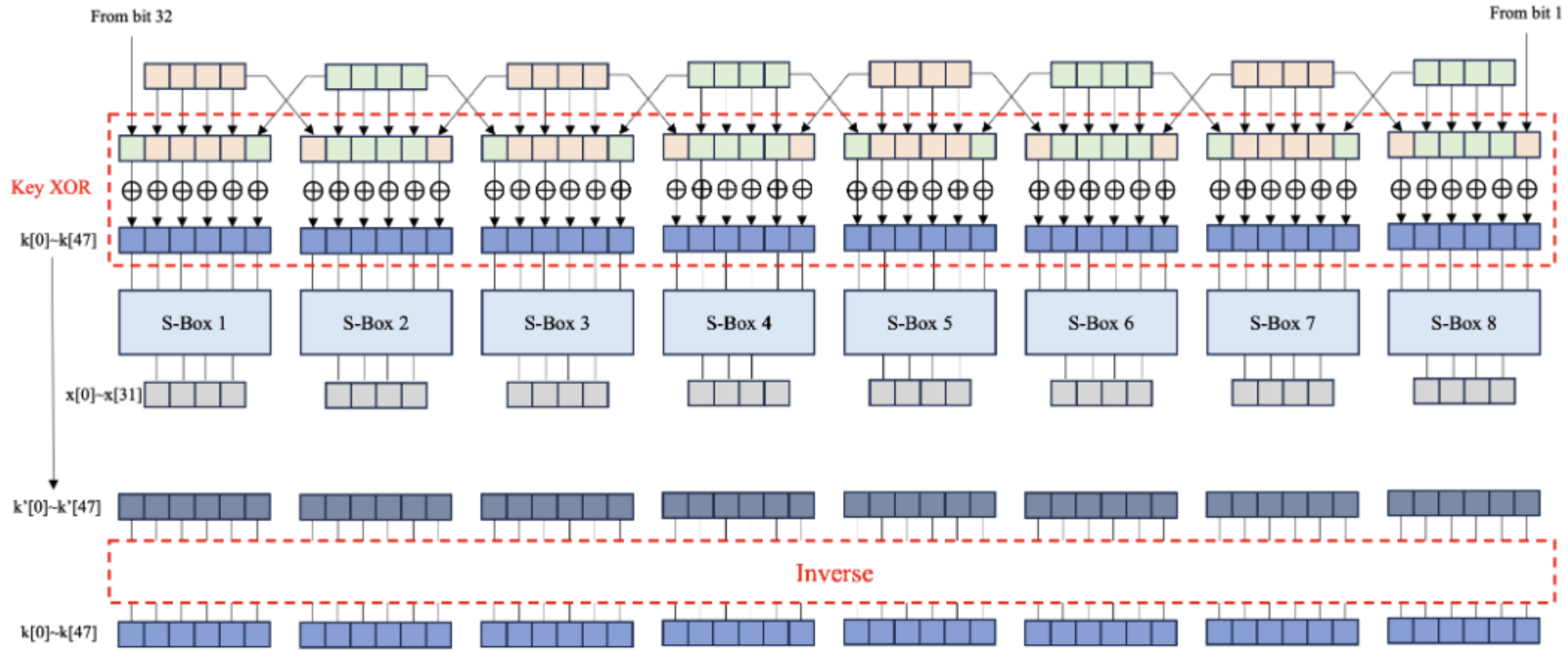


Figure 5. The Type A expansion P-Box.

Expansion P-Box

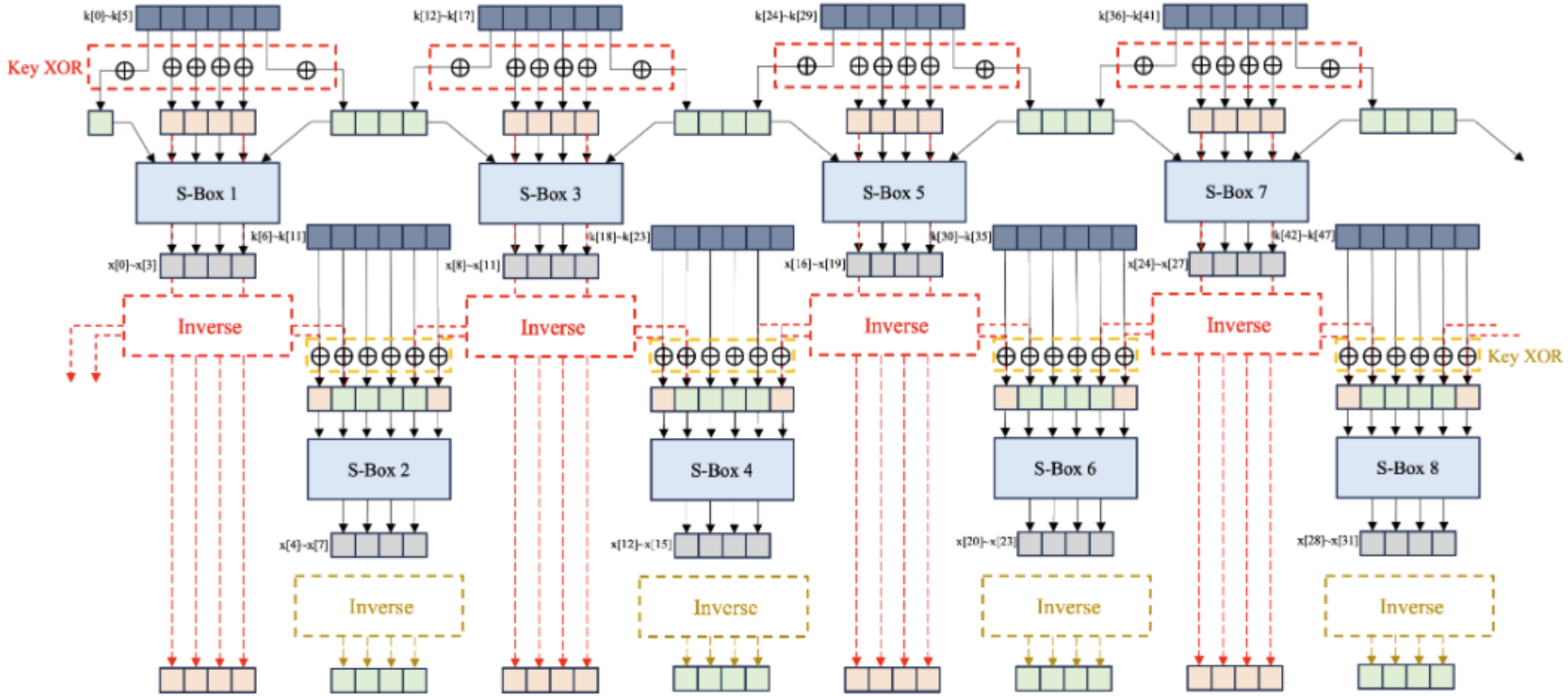


Figure 6. The Type B expansion P-Box.

TDES 양자회로 자원 추정결과 (Depth optimized)

S-Box (version 1)

Function		Quantum resources						
S-Box	P-Box	Qubit (M)	Toffoli depth (TD)	Toffoli	CNOT	1qCliff	Depth	$TD \cdot M$
Basic	Basic	7,536	1,024	3,424	12,992	7,184	1,044	7716864
	A	7,280	1,024	3,424	12,480	7,184	1,044	7454720
	B	7,280	1,952	3,424	12,480	7,184	1,661	14210560
A	Basic	943	6,848	6,848	20,672	11,232	13,893	6457664
	A	687	6,848	6,848	20,160	11,232	13,893	4704576
	B	687	6,848	6,848	20,160	11,232	13,892	4704576
B	Basic	1,328	1,024	6,848	20,672	11,232	2,162	1359872
	A	1,072	1,024	6,848	20,160	11,232	2,192	1097728
	B	1,072	1,952	6,848	20,160	11,232	2,982	2092544

S-Box (version 2)

Function		Quantum resources						
S-Box	P-Box	Qubit (M)	Toffoli depth (TD)	Toffoli	CNOT	1qCliff	Depth	$TD \cdot M$
Basic	Basic	6,896	1,024	3,536	11,536	7,600	1,012	7061504
	A	6,640	1,024	3,536	11,024	7,600	1,011	6799360
	B	6,640	2,016	3,536	11,024	7,600	1,468	13386240
A	Basic	936	7,072	14,080	33,856	21,888	29,314	6619392
	A	680	7,072	14,080	33,344	21,888	29,312	4808960
	B	680	7,072	7,072	17,856	11,456	14,772	4808960
B	Basic	1,328	1,024	13,246	36,636	20,316	4,034	1359872
	A	1,072	1,024	13,246	36,124	20,316	4,064	1097728
	B	1,072	2,016	6,848	20,160	11,232	2,982	2161152

TDES 양자회로 자원 추정결과 (Qubit optimized)

S-Box(.ver 1)

Function		Quantum resources						
S-Box	P-Box	Qubit (M)	Toffoli depth (TD)	Toffoli	CNOT	1qCliff	Depth	$TD \cdot M$
Basic	Basic	816	2,048	6,848	20,160	11,232	2,162	1671168
	A	560	2,048	6,848	19,648	11,232	2,192	1146880
A	Basic	936	13,696	14,080	33,856	21,888	29,314	12819456
	A	680	13,696	14,080	33,344	21,888	29,312	9313280
	B	680	6,848	7,072	17,856	11,456	14,772	4656640
B	Basic	1,288	2,048	13,444	32,262	18,598	4,322	2637824
	A	1,032	2,048	13,440	31,744	18,592	4,352	2113536
	B	1,032	1,952	7,072	17,856	11,456	2,843	2014464

S-Box(.ver 2)

Function		Quantum resources						
S-Box	P-Box	Qubit (M)	Toffoli depth (TD)	Toffoli	CNOT	1qCliff	Depth	$TD \cdot M$
Basic	Basic	776	2,048	7,072	17,856	11,104	2,354	1589248
	A	520	2,048	7,072	17,344	11,104	2,384	1064960
A	Basic	1,288	14,144	13,412	32,262	20,074	4,386	18217472
	A	680	14,144	14,080	33,344	21,472	29,888	9617920
	B	680	7,072	7,072	17,856	11,104	15,076	4808960
B	Basic	1,288	2,048	13,412	32,262	20,074	4,386	2637824
	A	1,032	2,048	13,408	31,744	20,064	4,416	2113536
	B	1,032	2,016	7,072	17,856	11,104	2,907	2080512

S-Box - ANF

Function	Quantum resources				
	Qubit	Toffoli	CNOT	1qCliff	Depth
S-Box1	63	32	85	75	60
S-Box2	56	29	77	56	43
S-Box3	57	27	86	66	52
S-Box4	42	17	69	30	47
S-Box5	62	29	91	61	65
S-Box6	57	26	85	51	52
S-Box7	57	29	80	57	67
S-Box8	54	25	79	53	59
Total	448	214	652	449	67

Table 4. Estimation of quantum resources for S-Box quantum circuits composed of standard gates.

Function	Quantum resources				
	Qubit	Toffoli	CNOT	1qCliff	Depth
S-Box1	56	32	72	77	65
S-Box2	50	28	66	57	63
S-Box3	53	28	75	60	47
S-Box4	39	18	63	43	53
S-Box5	56	30	78	63	64
S-Box6	53	31	66	62	74
S-Box7	51	27	72	56	52
S-Box8	50	27	69	57	68
Total	408	221	561	487	74

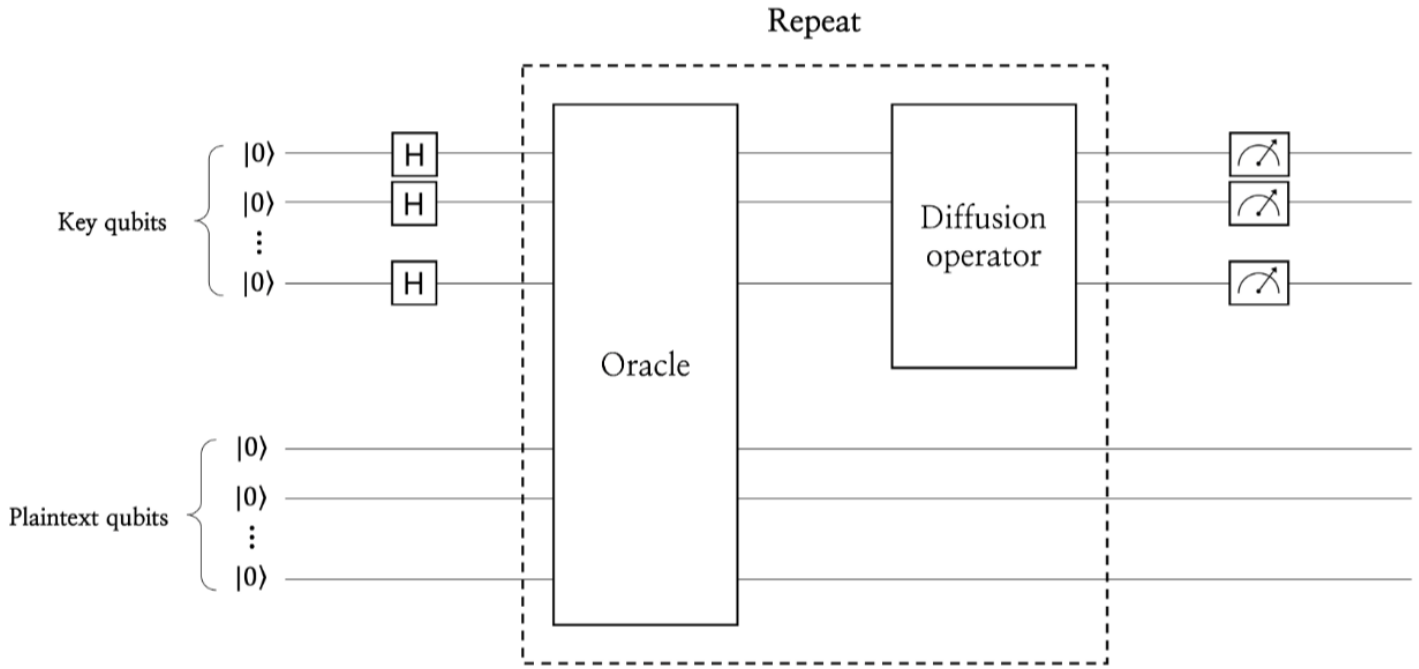
Table 5. Estimation of quantum resources for S-Box quantum circuits composed of non-standard gates.

DES vs AES (양자회로 자원비교)

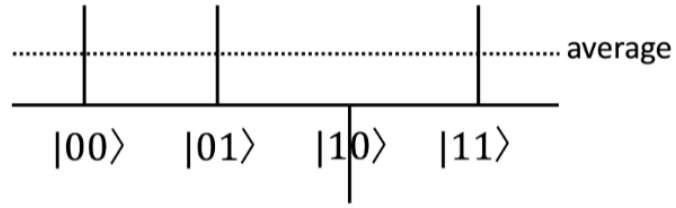
	Qubit	1qCliff	Depth	$Td \times M$
DES (optimized-qubit)	560	11,232	2192	1,146,880
AES-128	3428	138,148	731	548,480
AES-192	156,008	21,272	874	719,616
AES-256	191,772	26,607	1025	904,064

Grover's Algorithm

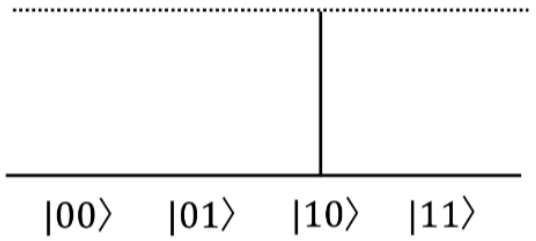
- **중첩 상태의 key를 이용하여 대칭키 암호에 대하여 전수조사를 수행하는 양자 알고리즘**
  - **Oracle :** 주어진 평문-암호문 쌍에 대한 키를 반환 **(공격 대상의 암호화가 양자 회로로 구현되어야 함)**
  - **Diffusion operator :** Oracle에서 반환한 키의 진폭을 증폭시켜 관측 확률 증가
  - **반복횟수:** $\left\lfloor \frac{\pi}{4} N \right\rfloor$ **,** N**= search space**



<Grover key search 회로 구조>



<Oracle>



<Diffusion operator>

TDES vs AES (Grover 자원 비교)

Algorithm	Quantum resources					
	Qubit	Toffoli	CNOT	1qCliff	Toffoli depth *(TD)*	Depth
TDES (depth-optimized)	-	1.17×2^{96}	1.58×2^{99}	1.09×2^{99}	1.17×2^{96}	1.16×2^{96}
TDES (qubit-optimized)	520	1.01×2^{99}	1.24×2^{100}	1.59×2^{99}	1.17×2^{97}	1.37×2^{97}
AES-128 [13]	3,429	N/A	N/A	N/A	N/A	1.121×2^{74}
AES-192 [13]	7,305	N/A	N/A	N/A	N/A	1.34×2^{106}
AES-256 [13]	7,817	N/A	N/A	N/A	N/A	1.572×2^{138}

[13] Jang, Kyungbae, et al. "Quantum analysis of AES." *Cryptology ePrint Archive* (2022).

Q & A