

# 다치양자논리에 의한 다중제어 Toffoli 게이트의 실현

## Realization of Multiple-Control Toffoli gate based on Multiple-Valued Quantum Logic

박동영\*

Dong-Young Park\*

### 요 약

다중제어 Toffoli(multiple-control Toffoli, MCT) 게이트는 원시 게이트에 의존적인 양자 기술을 필요로 하는 매크로 레벨 다치(multiple-valued) 게이트이며, Galois Field sum-of-product(GFSOP)형 양자논리 함수의 합성에 사용되어 왔다. 가역 논리는 저전력 회로 설계를 위한 양자계산(quantum computing, QC)에서 매우 중요하다. 본 논문은 먼저 GF4 가역 승산기를 제안한 후 GF4 승산기 기반의 quaternary MCT 게이트 실현을 제안하였다. MCT 게이트 실현을 위한 비교에서 제안한 MCT 게이트가 다중제어 입력이 증가할수록 종전의 작은 MCT 게이트 합성 방법보다 원시 게이트 수와 게이트 지연을 상당량 줄일 수 있음을 보였다.

### Abstract

Multiple-control Toffoli(MCT) gates are macro-level multiple-valued gates needing quantum technology dependent primitive gates, and have been used in Galois Field sum-of-product (GFSOP) based synthesis of quantum logic circuit. Reversible logic is very important in quantum computing for low-power circuit design. This paper presents a reversible GF4 multiplier at first, and GF4 multiplier based quaternary MCT gate realization is also proposed. In the comparisons of MCT gate realization, we show the proposed MCT gate can reduce considerably primitive gates and delays in contrast to the composite one of the smaller MCT gates in proportion to the multiple-control input increase.

Key words: multiple-control Toffoli(MCT) gate, multiple-valued, reversible circuit, GF4 multiplier, Galois Field sum-of-product(GFSOP)

### I. 서 론

가장 잘 알려진 전통적 양자 계산(quantum computation, QC)은 바이너리 논리이다[1]. 그러나 QC를 위해 바이너리에 대응할 만한 다치(multiple-valued,  $r \geq 3$ ) 논리는 양자 암호화를 위한 보안성[2],[3], 더욱 강력한 양자정보처리[4], 바이너리

실현에 비해  $1/\log_2 r$  배의 양자 레지스터 면적 감소의 이점을 제공하는 양자 메모리의 이점[5] 측면에서 바이너리 보다 강력한 미래의 대안 기술이다. 따라서 다치 암호화 실현은 대응하는 바이너리 실현보다 더 간결하며, 이와 같은 이점은 연구자들로 하여금 유용한 다치 양자논리 방법을 개발하게끔 만들고 있다.

1-qudit(quantum-digit)과 2-qudit 게이트의 양자 실

\* 강릉원주대학교 정보통신공학과(Dept. of Information & Telecommunication Eng., Gangnung-Wonju National University)

· 제1저자 (First Author) : 박동영

· 투고일자 : 2011년 12월 26일

· 심사(수정)일자 : 2011년 12월 26일 (수정일자 : 2012년 2월 22일)

· 게재일자 : 2012년 2월 28일

현은 전류 기술[6],[7]의 이용으로 가능하지만 일반적으로  $n$ -qudit ( $n>2$ ) 게이트는 두 입자들보다 더 많은 상호작용의 제어가 거의 불가능하기 때문에 양자 기술로 실현이 매우 어렵다. 그러므로 이들 게이트는 1-qudit과 2-qudit 게이트를 정점으로 실현되며, 이들은 매크로레벨(macro-level) 게이트라 불려진다. 대표적인 매크로레벨 게이트로는 Feynman과 Toffoli 게이트가 있으며, 이들은 원시(primitive) 게이트에 의존적인 기술의 정점에서 실현이 요구된다.

가장 잘 제안된 다치양자 원시게이트는 액체 이온 트랩(ion-trap)으로 실현 가능한 Muthukrishnan -Stroud (M-S) 게이트류이다[7]. 1-qudit과 M-S 게이트를 정점으로 하는 ternary Feynman과 3-입력 MCT 게이트의 실현[8]에서는 Feynman 게이트 실현에는 4개의 원시 게이트가 요구되며, Toffoli 게이트 실현에 부속 입력선 없이 16 개의 원시 게이트가 요구된다. 1-qudit과 M-S 게이트를 정점으로 하는 quaternary Feynman과 3-입력 MCT 게이트의 실현[8],[9]에서는 Feynman 게이트 실현에 6개의 원시 게이트가 요구되며, MCT 게이트 실현에는 부속 입력 상수의 재생성 없이 한 개의 부속 입력 상수와 30 개의 원시 게이트가 요구된다. 한편 가변 임계값을 갖는 수정된(modified) M-S(이하, mM-S) 게이트에 의한 1-qudit과 M-S 게이트를 정점으로 하는 quaternary Feynman과 3-입력과 4-입력 Toffoli 게이트의 실현은 [10]-[13] 등에 제시되어 있는데, 이 방법은 14 개의 원시 게이트와 2개의  $(n-1)$ 입력 MCT 게이트가 요구되어 입력  $n$ 이 증가할수록 원시게이트 수가 두 개의 하위 MCT 게이트 크기에 비례하여 증가한다.

본 논문에서는 1-qudit과 M-S 게이트를 정점으로 하는 모듈 구조의 2-입력 GF4 가역 승산기와 이를 확장한  $n$ -입력 MCT 게이트의 모듈구조 설계 방법을 제안한다. 본 논문의 기여는  $n$ -입력 확장 시에 부속 입력 없이 기존 방법들보다 원시게이트 수와 게이트 지연을 하위계층 MCT 게이트에 독립적인 모듈 구조 설계 방법의 제안에 있다.

본 논문의 구성은 2장에서 quaternary 양자 논리의 일반적 성질을 논하고, 3장에서 quaternary 양자 논리의 게이트 실현을 위한 기본 게이트로서 M-S 게이트와 mM-S 게이트를 정의한 후 최근의 양자 게이트 실현과 관련 연구를 고찰하였다. 4장에서는 본 논문에서 제안한  $n$ -입력 MCT 게이트의 설계 및 실현 방법을 논하였다. 5장에서는 최근의 관련 연구들과 원시 게이트 수와 게이트 지연 비교를 하였고, 6장에서 결론을 논하였다.

## II. Quaternary 양자 논리

임의 변수 수가  $n$ 인  $r$ 치 다치양자논리 함수의 가능한 함수 수  $N$ 은 식 (1)과 같다.

$$N = r^{(r^n)} \tag{1}$$

따라서  $r=4$  및  $n=1$ 인 quaternary 양자논리에서는 표 1과 같이 총 256개의 1-qudit 함수들이 존재한다.

표 1. 1-qudit 함수  
Table 1. 1-qudit functions.

X	256 경우의 quaternary 1-qudit 함수														
0	0	0	0	0	0	...	0	...	1	...	2	...	3	...	3
1	0	0	0	0	0	...	1	...	0	...	3	...	2	...	3
2	0	0	0	0	1	...	2	...	3	...	0	...	1	...	3
3	0	1	2	3	0	...	3	...	2	...	1	...	0	...	3

표 2. 24개 1-qudit 함수의 quaternary GFSOP 표현.  
Table 2. Quaternary GFSOP expressions to 24 1-qudit functions.

x	x	x+1	x+2	x+3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0
<hr/>				
x	2x	2x+1	2x+2	2x+3
0	0	1	2	3
1	2	3	0	1
2	3	2	1	0
3	1	0	3	2
<hr/>				
x	3x	3x+1	3x+2	3x+3
0	0	1	2	3
1	3	2	1	0
2	1	0	3	2
3	2	3	0	1
<hr/>				
x	x <sup>2</sup>	x <sup>2</sup> +1	x <sup>2</sup> +2	x <sup>2</sup> +3
0	0	1	2	3
1	1	0	3	2
2	3	2	1	0
3	2	3	0	1
<hr/>				
x	2x <sup>2</sup>	2x <sup>2</sup> +1	2x <sup>2</sup> +2	2x <sup>2</sup> +3
0	0	1	2	3
1	2	3	0	1
2	1	0	3	2
3	3	2	1	0
<hr/>				
x	3x <sup>2</sup>	3x <sup>2</sup> +1	3x <sup>2</sup> +2	3x <sup>2</sup> +3
0	0	1	2	3
1	3	2	1	0
2	2	3	0	1
3	1	0	3	2

본 논문에서는 다치양자논리의 기본으로 quaternary Galois Field(QGF 또는 GF4)를 고려하였다. 표2는 표1의 256개 1-qudit 함수들 중에서 특히 0,1,2,3의 순환적 연산 특성을 갖는 24개 quaternary 1-qudit 함수들로서 다치양자논리 함수의 GFSOP 합성에 매우 유용한 함수들이다. 표2 상의 모든 GF4 연산은 4차 원소집합  $Q=\{0,1,2,3\}$ 의 임의 두 원소간의 가산(기호  $+$  또는  $\oplus$ )과 승산(기호  $\cdot$  또는  $\otimes$ )이 표3을 만족하는 대수체이다.

표 3. GF4 가산과 승산.

Table 3. Addition and multiplication on GF4.

+	0	1	2	3	•	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	0	3	2	1	0	1	2	3
2	2	3	0	1	2	0	2	3	1
3	3	2	1	0	3	0	3	1	2

### III. Quaternary 양자 게이트 실현과 관련 연구

#### 3-1 QGFSOP 표현 함수의 성질

a,b,c,d가 서로 다른 고유한 quaternary 수이며  $g, h \in \{a,b,c,d\}$  일 때 가산 게이트는  $+g$ 로 표기한다. 이제 표2의 24개 1-qudit 함수 중에서 임의의 한 1-qudit 함수 A를  $A=\langle abcd \rangle$ 로 표기하면 입력 신호 A가 가산게이트  $+g$ 를 통과하면 a,b,c,d 각 원소에 대해  $+g$ 의 GF4 가산 연산을 실행한다. A에 대한 교환 연산은  $gh$ 로 표기하며, 입력 신호 A가  $gh$ 를 통과하면  $A=\langle abcd \rangle$ 에서 g에 대응하는 원소는 h로 그리고 h에 대응하는 원소는 g로 각각 치환된다. A에 대한 승산 연산은  $\times g$ 로 표기하며, 입력 신호 A가 g를 통과하면 a,b,c,d 각 원소에 대해  $\times g$ 의 GF4 승산 연산을 실행한다. 1-qudit quaternary 게이트의 Z변환은 표4와 같다.

표4. 1-qudit quaternary 게이트의 Z변환.

Table 4. Z transformation of 1-qudit quaternary gates.

입력 A	Z={+g, gh, ×g} 변환						
	+1	+2	+3	12	23	×2	×3
0	1	2	3	0	0	0	0
1	0	3	2	2	1	2	3
2	3	0	1	1	3	3	1
3	2	1	0	3	2	1	2

표4의 게이트들은 원시 게이트로 실현이 가능하다. 그림 1은 액체 이온트랩 양자기술로 실현 가능한 2-qudit quaternary M-S 게이트이다[7]-[9].c

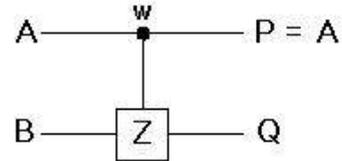


그림1. 2-qudit quaternary M-S 게이트.

Fig.1 2-qudit quaternary M-S gate.

그림 1의 M-S 게이트는 r차 경우에  $w=r-1$ 일 때 임의의 1-qudit 함수 입력 B에 대하여 표4의 Z 변환을 실시하고, 그 외의  $w \neq r-1$ 인 경우에 대해  $Q = B$ 를 실행한다. 따라서 quaternary 양자논리에서는  $A=3$ 인 경우에 한하여 표4의 Z변환을 실시하게 된다.

Khan[10] 등은 고정 임계값을 갖는 M-S 게이트를 확장해 가변 임계값 g에 대해 Z변환을 실행하는 수정된 M-S(modified M-S, 이하 mM-S) 게이트를 제안하였다.

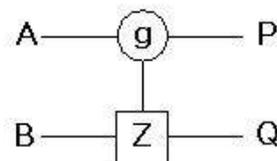


그림 2. mM-S 게이트.

Fig.2. mM-S gate.

그림2는 그림3과 같이 원시게이트에 의한 실현이

가능한데, quaternary 경우에 가산게이트 +U와 +V는 각각  $A+U=3$ 과  $3+V=A$ 의 GF4 연산을 만족하는 표5를 따른다.

표 5 mM-S 게이트 임계값.

Table5. Threshold to mM-S gate.

임계값 g	U	V
0	3	3
1	2	2
2	1	1
3	0	0

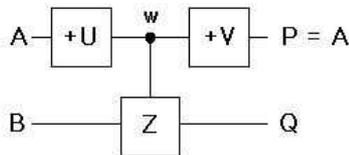


그림 3. mM-S 게이트 실현.  
Fig.3. Realization of mM-S gate.

한편 그림 4는 quaternary Feynman 게이트이며, 그림5는 그림 4의 원시게이트 실현이다.

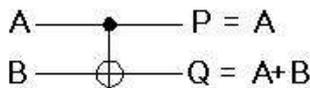


그림 4. Quaternary Feynman 게이트.  
Fig.4. Quaternary Feynman gate.

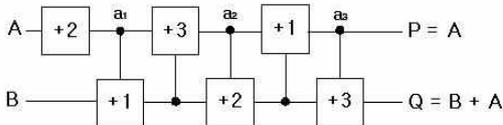


그림 5. Realization of quaternary Feynman 게이트.  
Fig.5. Realization of quaternary Feynman gate.

그림 6은 3-입력 quaternary MCT 게이트이다.

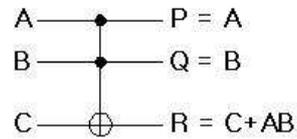


그림 6. 3-입력 quaternary MCT 게이트.  
Fig.6. 3-input quaternary MCT gate.

입력이 3-qudit 함수인 3-입력 quaternary MCT gate는 다양한 방법들로 실현되었다. Khan[8]은 종속 3단 구조로 27개의 가산게이트와 3개의 승산게이트 등 30개의 원시게이트로 3-입력 MCT 게이트는 실현하였다. Khan[11]에서는 3-입력 quaternary MCT 게이트를 그림 7과 같이 2 개의 2-입력 Toffoli(일명, Feynman) 게이트(점선)와 7개의 mM-S 게이트로 실현하였다.

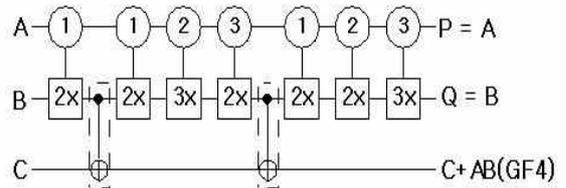


그림 7. 3-입력 quaternary MCT 게이트.  
Fig.7. 3-input quaternary MCT gate.

그림 7에 대한 Khan[12]의 원시게이트 실현은 그림 8과 같다.

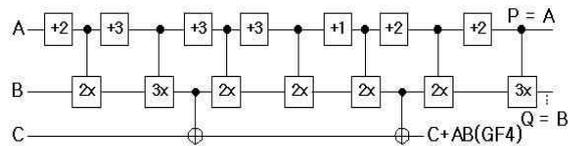


그림 8. 3-입력 quaternary MCT 게이트 실현.  
Fig.8. Realization of 3-input quaternary MCT gate.

결과적으로 Khan[11],[12] 등은 그림 8에서 총 26개의 원시게이트를 사용함으로써 Khan[8]보다 4개의 원시게이트를 줄일 수 있었다.

#### IV. 4-입력 quaternary MCT 게이트

그림 7과 같은 작은 MCT 게이트에 의한 큰 MCT 게이트 합성실현 방법[11]-[13]들은 3-입력에서 4-입력으로 확장할 때 두 개의 2-입력 MCT 게이트를 3-입력 MCT 게이트로 확장해야만 한다. 이 방법들은 두 개의 cascade된 3-입력 MCT 게이트들로 합성된 4-입력 MCT 게이트를 실현할 경우에 근본적으로 입력 수  $n$ 에 대해 하위 계층인 두 개의  $(n-1)$ 입력 MCT 게이트에 종속적이며,  $n$ 이 증가할수록 소요 원시게이트 수가 급증하게 된다. 이를 개선하기 위해 본 논문에서는  $n$  입력 증가 시에 하위계층 MCT 게이트에 독립적인 모듈 구조의  $n$ -입력 MCT 게이트를 제안한다.

4-1 mM-S 게이트를 이용한 GF4 승산기 설계

모듈 구조  $n$ -입력 MCT 게이트의 기본 원소모듈을 구성할 2-입력 GF4 승산기를 mM-S 게이트로 실현하면 그림 9와 같다.

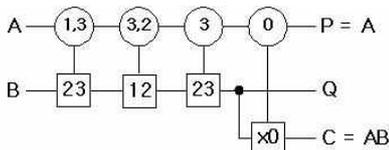
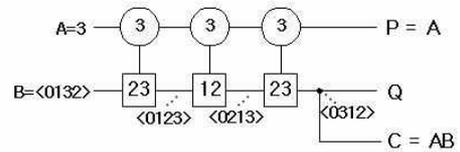
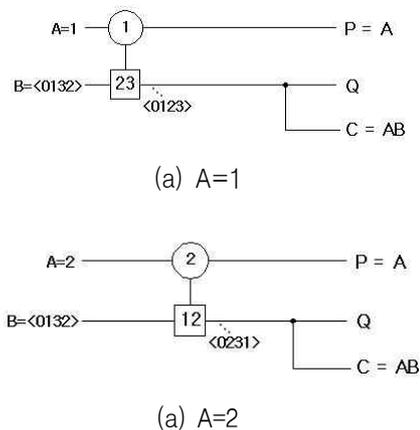


그림 9. 본 논문이 제안하는 GF4 비가역 승산기. Fig.9. A proposed irreversible GF4 multiplier in this paper.

그림10은  $B=\langle 0132 \rangle$ 일 때 입력 A에 대한 그림 9 승산기의 동작 흐름도이다.



(a) A=3  
그림 10. 그림9의 신호 흐름도. Fig.10. Signal flows on Fig.9.

그림 9에서 quaternary 입력  $A=0$ 인 경우는  $C=0$ 이다. 그림 10에서 영이 아닌 quaternary 입력  $A=1,2,3$ 에 대해  $P=A$ 이지만  $Q \neq B$ 이므로 그림 9는 비가역 출력 특성을 보임을 알 수 있다.

4-2 GF4 가역 승산기 설계

그림 9에 대한 가역 승산기로의 확장은 그림 11과 같은 대칭구조 설계에 의해 가능하다. 이제 그림 11은 모든 입력 A에 대해  $P=A$ 와  $Q=B$ 의 쌍방향 가역 특성을 갖는다.

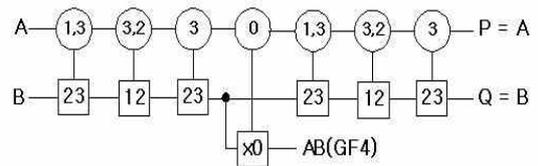


그림 11. 제안한 2-입력 GF4 가역 승산기. Fig.11. A proposed two-input reversible GF4 multiplier.

제안한 GF4 가역 승산기를 이용한 3-입력 MCT 게이트의 원시게이트 실현은 그림 11의 출력 단에 한 개의 Feynman 게이트 추가를 통해 그림 12와 같이 실현할 수 있다.

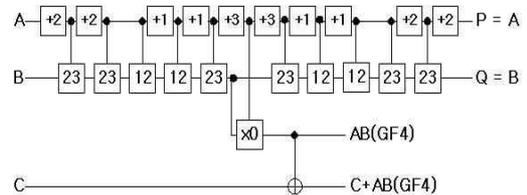


그림 12. 제안한 3-입력 Toffoli 게이트 실현. Fig.12. A proposed realization of 3-input quaternary MCT gate.

그림 12와 같이 본 논문은 3-입력 MCT 게이트를 21개의 원시게이트와 1개의 Feynman 게이트(원시게이트 6개)를 사용함으로써 총 27개의 원시게이트로 실현할 수 있었다.

4-3 GF4 가역승산기 모듈 구조의 MCT 게이트

그림 11의 2-입력 GF4 가역 승산기를 다음과 같은 모듈 구조로 정의한다.

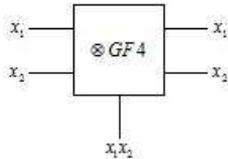


그림 13. 2-입력 GF4 가역 승산기 모듈.  
Fig.13. 2-input reversible GF4 multiplier module.

그림 13의 모듈 구조를 이용하여 4-입력 MCT 게이트를 실현하면 그림 14와 같다.

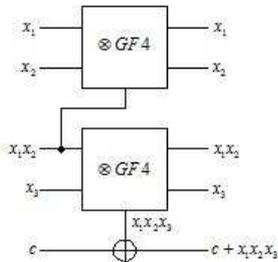


그림 14. 4-입력 MCT 게이트의 실현.  
Fig.14. A realization of 4-input MCT gate.

이제 그림 13의 모듈 구조를 확장한 n-입력 MCT 게이트의 실현은 그림 15와 같다.

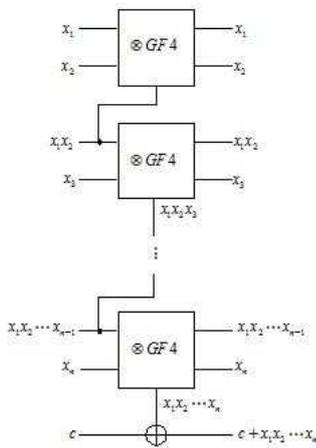


그림 15. n-입력 MCT 게이트의 실현.  
Fig.15. A realization of n-input MCT gate.

위에서와 같이 본 논문이 제안한 n-입력 MCT 게이트는 근본적으로 하위 계층의 MCT 게이트에 독립적인 모듈 구조를 갖고 있음을 알 수 있다.

V. 비교 및 검토

본 논문에서는 제안한 MCT 게이트의 성능 비교를 위해 입력이  $3 \leq n$ 으로 다중제어입력의 확장이 가능한 Khan[9]-[13]의 MCT 게이트를 중심으로 게이트 지연과 소요 원시게이트 수 및 확장 용이성 등을 비교하였다.

Khan이 사용한 MCT 게이트는 근본적으로 작은 MCT 게이트로 큰 MCT 게이트를 합성하는 방법이다. 즉 기본 게이트에 두 개의 (n-1) MCT 게이트를 cascade하여 n-입력 MCT 게이트를 합성하는 방식이다. 먼저 제안한 방법과 Khan 방법의 MCT 게이트에 대한 원시게이트 지연 비교에서 Khan MCT 게이트의 최대 게이트 지연은 그림 7에서 A와 B의 4개 원시게이트를 통과한 신호가 두 개의 cascade된 2-입력 MCT 게이트를 통과하는 경로에서 발생한다. 따라서  $3 \leq i \leq n$ 인 i-입력 MCT 게이트의 원시게이트 지연을  $G_i$ 라 할 때 Khan의 MCT 게이트 지연은  $G_3=4+2 \times 6=16$ ,  $G_4=4+2 \times 16=36$ ,  $G_5=4+2 \times 36=76$ , ...,  $G_n=4+2G_{n-1}$  같이 하위 MCT 게이트에 종속적이며 i가 증가 할수록 게이트 지연이 비선형적으로 급증하게 된다. 한편 제안한 MCT 게이트 실현 방법에 대한 게이트 지연은 그림 12에서  $G_3=6+11=17$ 이며, 그림 14에서  $G_4=6+2 \times 11=28$ 이다. 이를 확장하면  $G_5=6+3 \times 11=39$ 이며,  $i=n$ 일 때  $G_n=6+11(n-2)$ 이므로 하위 MCT 게이트에 독립적인 선형적 특성을 보인다.

n-입력 MCT 게이트의 소요 원시게이트 수를  $T_n$ 이라 할 때 제안한 방법과 Khan 방법의 MCT 게이트 실현에 소요된 원시게이트의 함수 특성은 각각  $T_n=6+21(n-2)$  및  $T_n=14+2T_{n-1}$ 과 같으며, 이것은 앞선 게이트 지연에서 나타난 함수 특성과 유사한 특성을 보인다. 표 6은 제안한 방법과 Khan 방법에 대한 성능 비교 결과이다.

표6. 게이트 지연과 소요 게이트 수에 근거한 MCT 게이트 실현 비교 (a)  $G_i$  (b)  $T_i$

Table6. comparisons of MCT gate realization based on gate delays and required gate numbers. (a)  $G_i$  (b)  $T_i$

i	Khan[9]-[13]	제안 방법
	$G_i$	
3	16	17
4	36	28
5	76	39
...	...	...
n	$4+2G_{(n-1)}$	$6+11(n-2)$

(a)

i	Khan[9]-[13]	제안 방법
	$T_i$	
3	26	27
4	66	48
5	146	69
...	...	...
n	$14+2T_{n-1}$	$6+21(n-2)$

(b)

위의 성능비교 결과 Khan[10]-[13]에서 사용한 작은 MCT 게이트로 큰 MCT 게이트를 합성하는 방법은 하위 MCT 게이트에 종속적인 구조이므로 다중 제어입력  $i$ 가 증가 할수록 게이트 지연과 소요 게이트 수가 비선형적으로 급증하게 되는 고비용 구조인데 반해 제안한 방법은 하위 MCT 구조에 독립적인 선형적 특성의 저비용 구조임을 알 수 있다.

MCT 게이트의 확장성은 제안한 방법의 경우 모듈 구조이므로 모듈 추가를 통한 확장이 가능하고, Khan의 MCT 게이트도 내부에 포함된 두 개의 작은 MCT 게이트를 한 단계 큰 MCT 게이트로 확장함으로써 확장이 가능하여 두 방법 모두 용이한 확장 특성을 갖고 있다.

## VI. 결 론

본 논문에서는 암호성, 저전력, 양자 계산 및 DNA 계산 등과 같은 잠재적 응용 분야로 인해서 관심을 받고 있는 다치양자논리 함수에 기반한 GF4 가역

승산기를 제안하고, 제안한 승산기를 모듈로 이용하여 MCT 게이트를 실현하는 두 가지 방법을 제안하였다.

본 논문이 제안한 GF4 승산기는 가역 회로로 설계되어 양방향 연산이 가능하므로 저전력의 양자계산회로 등에 활용할 수 있다. 특히 제안한 승산기를 원소 모듈로 한 MCT 게이트 실현에서 기존의 Khan 등이 사용한 MCT 게이트와의 성능비교 결과는 확장성 측면에서는 두 방법 모두가 용이한 확장성을 보이고 있지만, 다중제어입력이 증가할수록 제안한 방법이 Khan 방법보다 게이트 지연과 소요 원시게이트 수 절감 측면에서 개선된 실험 결과를 나타냄을 알 수 있었다. 이것은 MCT 게이트 실현 시에 하위계층 MCT 게이트를 내포한 종속적 구조가 독립적인 구조보다 종속 게이트의 누적에 따른 하드웨어 성능과 비용 측면에서 불리한 고비용 구조가 될 수 있음을 시사한다.

본 연구와 관련한 차후 연구 과제는 제안한 GF4 승산기와 MCT 게이트를 이용한 quaternary GFSOP 함수의 합성과 저비용 mM-S 게이트의 실현 등이라 할 수 있다.

## 참 고 문 헌

- [1] M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
- [2] H. Bechmann-Pasquinucci, A. Peres, "Quantum cryptography with 3-state systems," *Phys. Rev. Lett.* 85, 2000.
- [3] M. Bourennane, A. Karlsson, G. Björk, "Quantum key distribution using multilevel encoding," *Phys. Rev. Lett.* A 64, 2001.
- [4] A.D. Greentree, S.G. Schirmer, F. Green, L.C.L. Hollenberg, A.R. Hamilton, R.C. Clark, "Maximizing the Hilbert Space for a finite number of distinguishable states," *Phys. Rev Lett.* 92, 2004.
- [5] A. Muthukrishnan, C.R. Stroud Jr., "Multivalued logic gates for quantum computation," *Phys. Rev. A* 62, 2000.
- [6] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Phys. Rev. Lett.* 74, 4091, 1995.

- [7] A. Muthukrishnan, C.R. Stroud Jr., "Multivalued logic gates for quantum computation," *Phys. Rev. A* 62, 2000.
- [8] Mozammel H.A. Khan, "Quantum realization of Quaternary Feynman and Toffoli gates," *4th International Conference on Electrical and Computer Engineering ICECE, 19-21 December, Dhaka, Bangladesh*, pp.157-160, 2006.
- [9] A.I. Khan, N. Nusrat, S.M. Khan, M. Hasan, and M.H.A. Khan, "Quantum realization of some ternary circuits using Muthukrishnan-Stroud gates", *proceedings of 37th International Symposium on Multiple-Valued Logic (ISMVL 2007)*, 14-16, Oslo, Norway, May 2007.
- [10] Khan M.M.M., Biswas A.K., Chowdhury S., Tanzid M., Mohsin K.M., Hasan M., and Khan A.I., "Quantum realization of some quaternary circuits," *TENCON 2008, IEEE Region 10 Conference*, pp.1-5, 2008.
- [11] Mozammel H. A. Khan, "Quantum Realization of Multiple-Valued Feynman and Toffoli Gates Without Ancilla Input," *Proc. of 39th IEEE Int. Symp. on Multiple-Valued Logic (ISMVL 2009)*, pp.103-108, 2009.
- [12] M.M.M. Khan, Ayan Kumar Biswas, Shuvro Chowdhury, Masud Hasan and Asif Islam Khan "Synthesis of GF(3) based Reversible/Quantum Logic Circuits Without Garbage Output," *Proc. of 39th IEEE Int. Symp. on Multiple-Valued Logic (ISMVL 2009)*, pp.98-102, 2009.
- [13] Ayan Kumar Biswas, Shuvro Chowdhury, Md. Mahmud Muntakim Khan, Masud Hasan and Asif Islam Khan, "Some Basic Ternary Operations Using Toffoli Gates along with the Cost of Implementation," *Proc. of 41th IEEE Int. Symp. on Multiple-Valued Logic (ISMVL 2011)*, Tuusula, Finland, May 23-25, pp. 142-146, 2011.

### 박 동 영 (朴東泳)



1980년 2월 : 인하대학교 전자공학과 (공학사)

1985년 8월 : 인하대학교 대학원 전자공학과(공학석사)

1995년 8월 : 인하대학교 대학원 전자공학과(공학박사)

1991년 9월~현재 강릉원주대학교 과학기술대학정보통신공학과 교수

관심분야 : MVL, VLSI, QC, 가역 회로, 데이터 변환 등.