논문 03-01-05

T-gate를 이용한 $GF(2^2)$상의 가산기 및 승산기 설계

A Design of an Adder and a Multiplier on $GF(2^2)$ Using T-gate

尹 炳 熙*, 崔 永 熙*, 金 興 壽*
Byoung-Hee Yoon*, Young-Hee Choi*, Heung-Soo Kim*

요 약

본 논문에서는 유한체 $GF(2^2)$상에서의 가산기와 승산기를 전류모드인 T-gate를 이용하여 설계하였다. 제시된 회로는 전류 모드에서 동작하는 T-gate의 조합으로 가산 연산과 승산 연산을 수행하는 연산기를 설계하였다. T-gate는 전류 미러와 전송 게이트로 구성되며 4치 T-gate를 설계, 이를 이용하여 $GF(2^2)$의 가산기와 승산기를 1.5um CMOS 공정을 사용하였다. 전원전압은 DC 3.3V이며 단위 전류는 15uA이다. 본 논문에서 제시한 전류 모드 CMOS 연산기는 T-gate의 배열에 의한 모듈성의 이점을 가지고 있으므로 다치 T-gate를 구현하여 다치 연산기를 쉽게 구현할 수 있게 하였다.

Abstract

In this paper, we designed a adder and a multiplier using current mode T-gate on $GF(2^2)$. The T-gate is consisted of current mirror and pass transistor, the designed 4-valued T-gate used adder and multiplier on $GF(2^2)$. We designed its under 1.5um CMOS standard technology. The unit current of the circuits is 15μA, and power supply is 3.3V VDD. The proposed current mode CMOS operator have a advantage of module by T-gate's arrangement, and so we easily implement multi-valued operator

Key word : T-gate, $GF(2^2)$, Adder, Multiplier

Ⅰ. 서 론

최근 2진논리에 근거한 집적회로 기술의 발전으로 회로의 형태가 VLSI, ULSI화되어 단일 칩상에 방대한 양의 회로를 집적할 수 있게 되었다. 그러나 단일 칩상에 방대한 양의 회로를 집적하기 위해서는 칩상의 상호 결선의 복잡성, 외부 단자의 증가와 연산속도의 제한성, 정보전송량의 방대함에 따른 정보전송시간지연등의 문제점들이 대두되기 시작했다. 이러한 문제점들을 해결하기 위하여 지난 수십 년 동안 다치 논리 회로의 실현에 많은 관심 가져왔으며[1-3], 그 중에서도 유한체(Galois Field; *GF*)는 2진 논리를 수행하는 부울체의 확장이라는 점에서 다치 논리 이론의 주관심 분야가 되었다[4,5].

유한체는 스위칭 이론, 오진 정정 부호, 디지털 신호처리 및 화상 처리, 디지털 통신의 암호화 및 해독화를 요하는 보안 통신 등에 많이 응용되고 있다. 특히,

* 仁荷大學校 電子工學科
(Department of EE, Inha Univ..)

接受日:2003年 3月 13日, 修正完了日: 2003年 7月 11日

$GF(2^m)$은 신호 처리와 화상 처리 분야에서 특별한 계산을 요하거나 범용 컴퓨터 계산의 고속화를 보조하는 고성능 전용 컴퓨터의 설계에 효과적이며, VLSI 설계에 응용되고 있다[6,7]. 유한체 $GF(p^n)$(단 $p \geq 3$)상에서 가산과 승산은 2진 산술 연산과는 현저하게 다르며 유용성과 단순성 때문에 유한체에 관한 연구가 활발히 진행되고 있다. 유한체상의 가산은 직접적이고 비트 독립적인 $mod(p)$ 연산으로 2진 가산보다 쉬운 반면에 승산은 2진 승산 보다 어렵고 복잡한 계산이 요구되나 단자당 높은 함수 기능 및 고밀도 실현의 장점을 가지고 있다[8,9].

초기의 다치 논리 회로의 설계는 주로 전압 모드 쌍접합 트랜지스터와 CMOS 회로에 의해 이루어져 왔다. 그러나 대부분의 전압 모드 다치 논리 회로는 회로의 복잡성과 전달 지연 때문에 2치 논리 회로와 경쟁이 못되어 새로운 기술인 전류 모드 CMOS 다치 논리 회로가 1980년대 중반에 소개되었다[10]. 본 논문에서 제시된 전류 모드 회로는 VLSI화의 요구 사항들에 대하여 호환성을 가지며, 적은 CMOS 공급 전압에서 안정하게 동작하며, 전압 모드가 갖는 결점을 보완하고 임의의 정점에서 전류 신호의 가감과 높은 전압의 공급 없이도 각 기수의 할당이 용이한 이점을 갖는다[11,12]. 또한 유한체상에서의 가산 및 승산 알고리즘이 제안되었으나 불행하게도 이 알고리즘은 불규칙한 회선 경로 선택, 복잡한 제어 문제, 비모듈화 구조 및 병발성(simultaneity)의 부족 때문에 VLSI 구조의 설계에 부적합하였다[13]. 이런 문제점들을 본 논문에서는 T-gate를 사용하여 회선 경로의 규칙성, 간단한 전류 제어, 모듈화 구조를 갖춘 GF(2^2)상에서의 가산기와 승산기를 설계하였다.

II. 전류 모드 T-gate 설계

전류모드회로는 정보를 전류로 표현하므로 공급전원의 크기를 증가할 필요가 없으며 가산, 감산 및 보수 연산을 쉽게 실현할 수 있고 전류비교가 바로 수행될 수 있으며 동작범위가 넓어서 큰 기수도 그리 큰 전원 전압의 공급 없이 실현된다.

2.1. 전류모드 CMOS 기본 회로

전류 모드 CMOS 기본 회로는 여러 논문을 통해서 많은 종류가 발표되어 왔다[8,9,].

본 절에서는 이들 중 본 논문에서 제시되는 회로들을 구성할 전류 모드 CMOS의 기본 회로들을 그림 1에서 보인다.

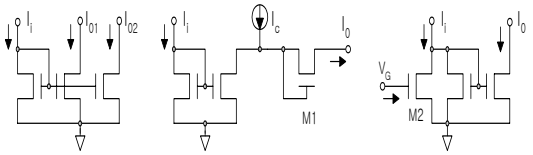


그림 1. 전류 모드 CMOS 기본 회로
(a) 전류 미러 회로
(b) 전류 차분 회로
(c) 전류 스위치 회로
Fig. 1 Current mode CMOS basic circuits.
(a) current mirror circuit
(b) current difference circuit
(c) current switch circuit

그림 1(a)는 하나의 입력 전류원에 대하여 소자 특성이 동일한 경우 여러 개의 출력 전류를 갖는 전류 미러 회로이다. 이는 일반적으로 전류 모드 회로에서 팬아웃 수가 1이라는 결점을 보완해 주며, 전류 이득에 관계되는 MOS 소자의 폭(W)과 길이(L)의 비율이 동일하다고 가정한 경우 출력 전류는 입력 전류와 같은 값을 갖게 된다[12].

그림 1(b)는 전류 차분 회로이며, 정전류원으로 표시되는 문턱전류 Ic가 P채널 MOS로 구성되며, M1 트랜지스터는 다이오드 특성을 나타낸다. 이 회로에 대한 동작 특성은 식 (1)과 같다.

$$I_0 = \begin{cases} I_C - I_i & iff \quad I_C > I_i \\ 0 & iff \quad I_C \leq I_i \end{cases} \qquad (1)$$

그림 1(c)는 전류 스위치 회로이며, 패스 트랜지스터 M2의 게이트 전압 V_G가 높게되면 출력 전류가 0이 되고 M2의 V_G가 낮게되면 전류 스위치 회로는 전류 미러 회로로 동작한다.

2.1 $GF(p^n)$상의 T-gate 설계

2진 시스템에서는 선택 신호로부터 정보를 선택하여 단일 출력으로 나타내는 멀티플렉서 회로를 사용한다.

그림 2에 4-to-1 멀티플렉서를 예를 들어 나타내었다.

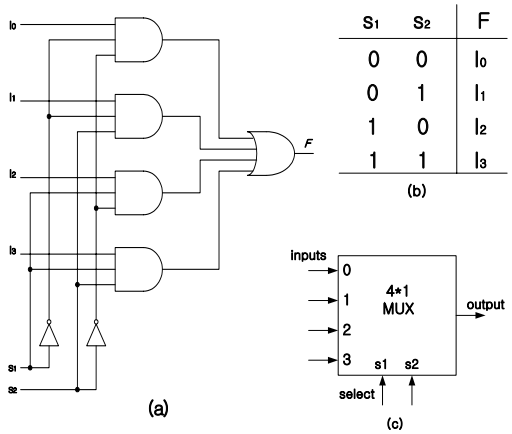
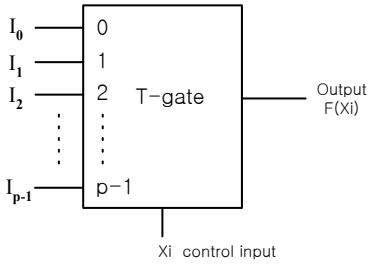


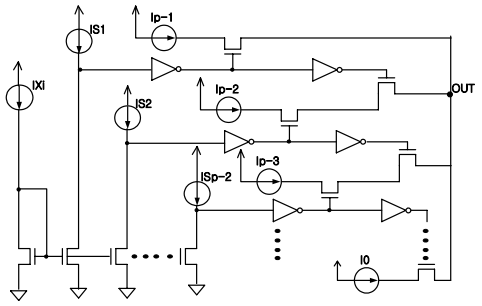
그림 2. 4-to-1 라인 멀티플렉서
(a) 논리다이어그램
(b) 함수표
(c) 블럭다이어그램

Fig. 2 4-to-1 Line Multiplexer
(a) Logic diagram
(b) Function table
(c) Block diagram

본 논문에 적용되는 다치 논리 시스템에서는 멀티플렉서와 같은 기능을 갖는 T-게이트를 사용한다. 입력단으로 들어오는 입력신호를 선택신호로부터 선택된 후 출력단으로 나가는 원리는 2진 시스템에서의 멀티플렉서와 같다. 그러나 멀티플렉서는 입력 비트수가 늘어날수록 선택신호의 비트수도 늘어나는 반면 본 논문에서 제안한 T-게이트는 입력개수와 무관하게 오직 하나의 선택신호를 갖는다. 그리고 본 논문에서 제안한 T-gate는 전류 모드로 구성하였다. 유한체 $GF(p^n)$상에서 일반적으로 사용할 수 있는 전류 모드 MOSFET에 의한 다치 T-gate는 그림 3과 같다.



(a)



(b)

그림 3. 전류 모드 MOSFET에 의한 p치 T-gate
(a) p치 T-gate 회로도
(b) 블럭다이어그램

Fig.3 p-valued T-gate using current mode MOSFET
(a) p-valued T-gate circuit
(b) Block diagram

위의 그림 3에서 전류 모드 MOSFET에 의한 T-gate의 출력 값 F는 다음 식(2)와 같다.

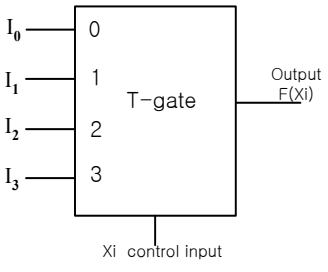
$$\begin{aligned} F(I_0, I_1, \cdots, I_{p-1} ; X_i) &= I_0 \quad (\text{if } X_i = 0) \\ &= I_1 \quad (\text{if } X_i = 1) \\ &= I_2 \quad (\text{if } X_i = 2) \\ &\vdots \\ &= I_{p-1} \quad (\text{if } X_i = p-1) \end{aligned} \tag{2}$$

여기서 $I_i \in GF(p^n)$이며, i는 $\{0,1,2,\cdots,p-1\}$이다.

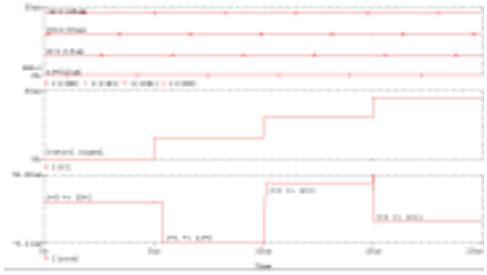
위 식(2)에서 p치 T-gate의 제어 신호 Xi(i=0,1,2,…,p-1)에 따라서 출력 F(Xi)는 제어 신호에 의해 I_0, I_1, …, I_{p-1}의 신호가 선택된다.

2.2 $GF(2^2)$상에서의 T-게이트 설계

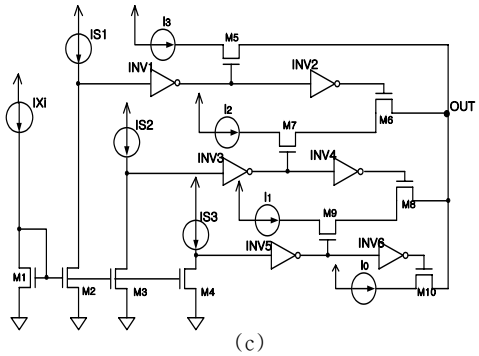
그림 4에서는 4치 T-gate 회로도를 나타내었고 그림 4-(c)에서는 4치 T-gate의 제어 신호에 따른 모의 실험 결과 파형을 나타내었다.



(a)



(b)



(c)

그림 4. 4치 T-게이트
(a) 블럭다이어그램
(b) 4치 T-게이트 회로도
(c) 모의 실험 결과
Fig. 4 4-valued T-gate
(a) Block diagram
(b) 4-valued T-gate circuit
(c) Simulation result

그림 4의 4치 T-gate는 전반적인 구성은 p치 T-gate와 같다. 여기서 단위 전류는 15uA를 사용하고 논리 0은 0uA, 논리 1은 15uA, 논리 2는 30uA, 논리 4는 45uA를 나타낸다. 하나의 예를 들면 선택신호가 논리 3(45uA)라면 각각 이 전류는 M2, M3, M4의 드레인에 전류가 복제되고 기준전류원 $I_{S1(45uA)}$, $I_{S2(30uA)}$, $I_{S3(15uA)}$와 인버터에 의해 패스트랜지스터 M5만 on이 되어 입력 전류 I_3만 출력 단자로 흐르게 된다. 그림 4의 (c)의 결과 파형에서 T-gate의 입력으로 들어가는 데이터(I0=30uA, I1=0uA, I2=45uA, I3=15uA)는 제어신호(0, 1, 2, 3)에 의해 입력 값이 선택되어 출력되어지는 것을 알 수 있다.

III. $GF(2^2)$상의 가산기와 승산기 설계

본 논문에서 제안된 4치 T-gate의 회로를 $GF(2^2)$상에서의 가산과 승산 연산을 수행하는 4치 가산기와 승산기를 설계하였다.

유한체 $GF(p^n)$상에서 $GF(2^2)$ p=2이고 n=2인 경우이다. 그러므로 $GF(2^2)$상의 원소들은

$$x^{pn}-x = x^4 - x$$
$$= x*(x-1)*(x^2 + x + 1) \quad (3)$$

로 분해되고 $x^2 + x + 1$은 기약 다항식이 된다. 따라서 $x^2 + x + 1 = 0$의 한 근을 α라 하면 $GF(2^2)$의 원소는 f1*α+f0의 형으로 표시된다. $GF(2^2)$의 원소는 표 1과 같다.

표 1. $GF(2^2)$의 원소표
Table 1 Elements of $GF(2^2)$

f_1*α	f_0	F(α)	기호
0*α	0	0	0
0*α	1	1	1
1*α	0	α	2
1*α	1	1+α	3

$GF(2^2)$의 원소들 {0, 1, α, 1+α}에 의한 가산표와 승산표는 다음 표 2와 같다.

표 2. $GF(2^2)$상에서의 가산과 승산 연산
Table 2. Addition and multiplication on $GF(2^2)$

y \ x	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

(a) (x+y)mod(4)

y \ x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

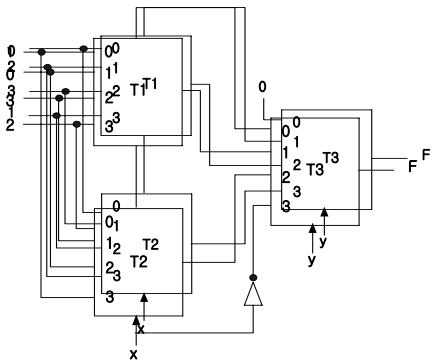
(b) (x*y)mod(4)

표 2에 의한 가산 연산과 승산 연산은 모듈러 연산을 수행하기 때문에 올림수가 발생하지 않는다.

4치 T-gate를 이용하여 표 2의 $GF(2^2)$ 가산과 승산을 구현한 회로는 다음의 그림 5와 그림 6과 같다.

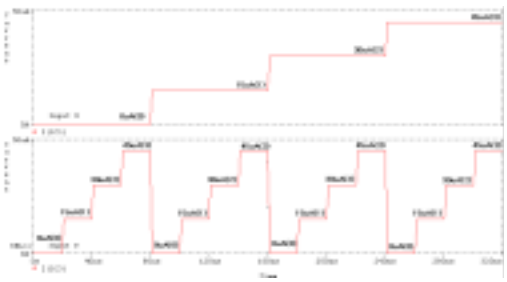
그림 5. $GF(2^2)$의 가산기
Fig. 5 Adder gate on $GF(2^2)$
그림 6. $GF(2^2)$의 승산기
Fig. 6 Multiplier on $GF(2^2)$

IV. 모의 실험 결과 및 결론

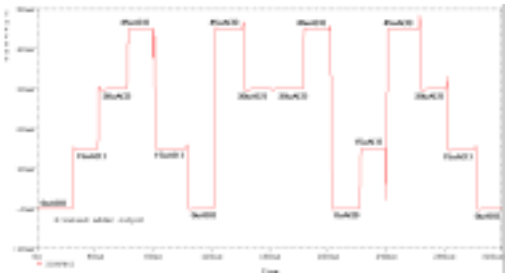


4.1. 모의 실험 결과

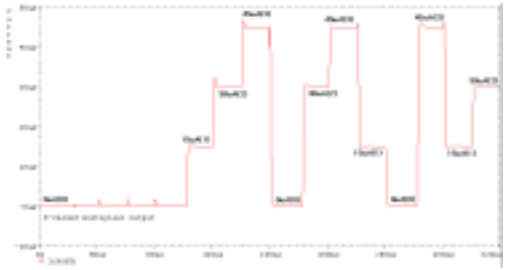
본 논문에서 제안된 $GF(2^2)$상에서의 가산기와 승산기의 모의 실험은 SPICE를 사용하여 수행하였으며 Level 3의 파라미터와 CMOS 1.5um 1-poly, 2-metal 공정에서 수행하였다. 다음 그림 7에서는 $GF(2^2)$상에서의 두 제어 신호 X, Y에 의한 가산 연산과 승산 연산을 수행한 결과를 나타내었다. 결과 파형은 표 2에 따른다.



(a)



(b)



(c)

그림 7. $GF(2^2)$상에서의 가산기와 승산기의 모의 실험
(a) 제어 신호 x, y
(b) 가산기의 출력 파형
(c) 승산기의 출력 파형

Fig. 7 Simulation of adder and multiplier on $GF(2^2)$
(a) Control signal x, y
(b) Simulation wave of adder
(c) Simulation wave of multiplier

다음 표 3은 본 논문에서 제안한 $GF(2^2)$에서의 가산기와 승산기, 그리고 각각의 T-gate 모듈회로의 모의 실험 결과를 나타내었다.

표 3. 모의실험 결과
Table 3 Simulation result

	Power dissipation	Delay in nsec (worst case)
4-valued T-gate	296㎼	1.4ns
4-valued adder	691㎼	2.6ns
4-valued Multiplier	691㎼	2.4ns

4.2 결 론

본 논문에서는 $GF(2^2)$상에서 다치 논리에 대한 가산기 및 승산기를 제안하였다. 제시된 전류 모드 MOSFETs에 의한 4치 연산기는 전류 모드로 동작하는 T-gate의 조합으로 이루어져있으며 입력 신호를 받아서 선택 신호에 의해 연산 결과를 출력하는 동작 특성을 나타내었다. 그리고 Spice 시뮬레이션을 통하여 이

회로들에 대하여 동작 특성을 보였다.

본 논문에서 설계된 가산기와 승산기를 사용하여 다치 시스템을 설계할 때 2진 시스템에서처럼 게이트(가산, 승산)의 배열로 구현할 수 있다. 그러므로 설계에 따라 모듈성을 갖는 T-gate를 배열하여 원하는 다치 시스템을 구현할 수 있게된다. 일반적으로 다치 시스템을 구현할 때 사용되는 구동방법은 전류모드를 사용하는데 그 이유는 전류모드가 다치 논리의 멀티레벨을 표시하기 용이하고 저전력과 고속의 데이터 처리 능력을 갖기 때문이다.

본 논문에서 제시한 전류 모드 MOSFETs에 의한 $GF(p^n)$상의 연산기에서 전류 모드 MOSFETs의 $mod(p)$ 승산 연산 회로는 $GF(2)$상에서는 전류원의 값만 변환하면 AND 게이트로 동작하고, $mod(p)$ 가산 연산 회로는 전류원의 값만 변환하면 XOR 게이트로 동작하므로 2치 논리 회로 및 다치 논리 회로에서 호환성을 갖는 장점이 있다.

제시된 회로들은 1.5㎛ CMOS 표준 기술을 사용하여 Spice 모의 실험을 하였다. p치 연산기의 단위 전류 I_u는 15㎂, VDD 전압은 3.3V를 사용하였으며 MOSFETs 모델 파라미터는 LEVEL 3을 사용하였다. 본 논문에서 제시한 전류 모드 MOSFET의 p치 연산 게이트는 회선 경로 선택의 규칙성, 간단성, 셀 배열에 의한 모듈성의 이점을 가지며, 특히 차수 n이 증가하는 유한체의 두 다항식의 가산 및 승산에서 확장성을 가지므로 VLSI화 실현에 적합할 것으로 생각된다.

향후 연구 과제는 산술논리연산기(ALU)에 적용하여 다치 산술논리연산기를 설계하는데 있다. 다치 산술논리연산기에서 입력 전류를 저장하는 다치 기억소자의 설계 및 구현이 필수적이며, 실용화를 위해서 전류 모드 동작에 의한 소비 전력 문제, 잡음에 대한 대책 및 미세 선폭의 반도체 기술에 맞도록 실제로 IC화하여 실용화하는 것이다.

참고 문헌

[1] K. C. Smith, "The Prospects for Multi-valued Logic : A Technology and Applications View," *IEEE Trans. on Comput*. vol. C-30. pp.619-634, 1981.

[2] T. Hanyu, M. Kameyama, T. Higuchi, "Prospects of Multiple-Valued VLSI Precessors," *IEICE Trans. Electron*, vol. E76-C, no.3, pp.383-392, March 1993.

[3] K. C. Smith, "Multiple-valued logic : A Tutorial and Appreciation," *COMP. mag.*, pp.17-27, April 1988.

[4] B.Benjauthrit and I. S. Reed, "Galois switching functions and their application," *IEEE Trans. Comput.*, vol. C-25, no.1, pp.78-86, Jan. 1976.

[5] K. S. Menger, "A transform logic networks," *IEEE Trans. Comput.*, vol. C-18, no.3, pp.241-250, Mar. 1969.

[6] C. C. Wang, T. K. Truong, H. M. Shao, L. J. Deutsch, J. K. Omura and I. S. Reed, "VLSI architectures for computing multiplications and inverses in GF(2^m)," *IEEE Trans. Comput.*, vol. C-34, no.8, pp.709-717, Aug. 1985.

[7] H. M. Shao, T. K. Truong, L. J. Deutch, J. H. Yaeh and I. S. Reed, "A VLSI design of a pipelining Reed-solomon decoder", *IEEE Trans. Comput.*, vol. C-34, no.5, pp.393-403, May 1985.

[8] Z. Zilic and Z. Vranesic, "Current-mode CMOS Galois field circuits," *Proc. 23th ISMVL*, Sacramento, CA, USA, pp.245-250, May 1993.

[9] S. P. Onneweer and H. G. Kerkhoff, "Current-mode CMOS high-radix circuits," *Proc. 16th ISMVL*, Blacksburg, Virginia, USA, pp.60-69, May 1986.

[10] K. Y. Fang and A. S. Wojcik, "Modular Decomposition of combinational Multiple-Valued circuits," *IEEE Trans. Comput.*, vol. 37, no.10, pp.1293-1301, Oct. 1988.

[11] George Epstein, "Multiple-valued logic design an introduction", *Institute of Physics Publishing*, 1993.

[12] T. Hanyu, S. Kazama, M. Kameyama, "Design and implementation of a Low-Power Multiple-Valued Current Mode Integrated Circuit with Current-Source Control", *IEICE Trans. Electron* vol. E80-C, no.7, pp.941-947, July 1997

[13] T.Uemura, T.Baba "Demonstration of a novel multiple-valued T-gate using multiple-junction surface tunnel transistors and its application to three-valued data flip-flop," *ISMVL 30th*, pp.305-310, May 2000

저 자 소 개

尹 炳 熙(學生會員)

1997년 2월 원광대학교 전자공학과 졸업(공학사)
1999년 2월 인하대학교 대학원 전자공학과 졸업(공학석사)
1999년 3월 ~ 현재 인하대학교 대학원 전자공학과 박사과정(박사수료)
주관심분야 : 다치 프로세서, 다치 저장 소자 설계, VLSI 설계

崔 永 熙(正會員)

1980년 2월 단국대학교 전자공학과 졸업(공학사)
1982년 8월 인하대학교 대학원 전자공학과 졸업(공학 석사)
1985년 3월 ~ 현재 재능대학 정보전자 계열 교수
2000년 3월 ~ 현재 인하대학교 대학원 전자공학과 박사과정(박사수료)
주관심분야 : 다치논리, VLSI 설계, SMPS

金 興 壽
제6권 1호 논문 02-01-04 참조
인하대학교 전자공학과 교수