논문 2010-47SC-1-4

새로운 패리티 보존형 가역 논리게이트

(New Parity-Preserving Reversible Logic Gate)

김 성 경*, 김 태 현**, 한 동 국***, 홍 석 희****

(Sung-Kyoung Kim, Tae Hyun Kim, Dong-Guk Han, and SeokHie Hong)

요 약

본 논문에서는 새로운 패리티 보존형 가역 논리게이트를 제안한다. 패리티 보존형 가역 논리게이트는 입력 값과 출력 값의 패리티가 같은 가역 논리게이트를 의미한다. 최근 가역 논리 게이트가 저전력 CMOS 디자인, 양자 컴퓨팅 그리고 나노 테크놀로지와 같은 분야에서 전력을 효율적으로 사용하는 방법임을 알려졌다. 그리고 패리티 체크(parity-checking)는 디지털 시스템에서 오류 주입을 확인 하는 대표적인 방법 중 하나이다. 제안하는 새로운 패리티 보존형 가역 논리게이트는 모든 boolean 함수를 구성할 수 있고, 기존의 오류 확인 boolean 함수보다 가역 논리게이트 수, garbage-output의 수 그리고 하드웨어 연산량에서 효율적으로 구성할 수 있다.

Abstract

This paper proposes a new parity-preserving reversible logic gate. It is a parity-preserving reversible logic gate, that is, the party of the outputs matches that of the inputs. In recent year, reversible logic gate has emerged as one of the important approaches for power optimization with its application in low CMOS design, quantum computing and nono-technology. We show that our proposed parity-preserving reversible logic gate is much better in terms of number of reversible logic gates, number of garbage-outputs and hardware complexity with compared ti the exiting counterpart.

Keywords : Reversible logic gate, parity-preserving, fault tolerant, quantum computing, nano-technology

Ⅰ. 서 론

Laundaner[1]은 비가역적인 연산과정에서 정보를 잃어버릴 때마다 엔트로피가 증가한다는 사실을 밝혀내었다. 즉, "Information Loss = Energy Loss"임을 주장하였다. 기존의 컴퓨터의 모든 Boolean 수식은 고정된 논리 게이트들의 집합으로 구성되어 있다. AND, OR 그리고 NOT 등은 가장 기본적인 게이트 집합이며, 이는 다대일(many to one) 연산이다. 이러한 연산은 논리적으로 가역적이지 않다.

고전적 가역 연산(Classical reversible computation)은 양자 컴퓨터의 개발의 기초가 되어 연구되었다. 컴퓨터의 사이즈를 최소화 하는데 가장 큰 문제인 열의 발산을 하지 않고 실행 될 수 있는 것은 모든 오퍼레이션들이 가역적(reversible)으로 실행될 경우이다. 이것을 논리적 가역성이라고 하고 디바이스가 거꾸로 실행 될 수 있다면 물리적 가역성이라고 부르게 된다. 논리적 가역성의 조건은 입력과 출력이 어느 쪽에서도 서로 검색 가능해야함이다. 이러한 논리적 가역성을 가지는 게

* 학생회원-주저자, **** 정회원, 고려대학교 정보경영공학전문대학원
(Graduate School of Information Management and Security, Korea University)
** 학생회원, 한국전자통신연구원(ETRI) 부설연구소 연구원
(The Attached Institute of ETRI)
*** 정회원-교신저자, 국민대학교 수학과
(Department of Mathematics, Kookmin University)
※ 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21 사업'의 지원비를 받았음.
접수일자: 2009년5월27일, 수정완료일: 2009년12월28일

이트를 가역 논리게이트(Reversible logic gate)라고 한다. 이러한 가역 논리게이트를 이용하여 저전력 CMOS(low-power CMOS)[2], 양자 컴퓨팅(quantum computing)[3], 나노 테크놀로지(nano-technology)[4]에 효과적으로 기술할 수 있게 된다.

디지털 로직 시스템에서 오류 주입을 확인하는 가장 대표적인 방법이 패리티 확인(parity checking)방법[10~11]이다. 가역 논리게이트에 일반적인 패리티 확인방법을 적용하는 경우 garbage-output(Ⅱ장. 정의 3 참조)의 수가 증가하면서 효율성과 안전성이 나빠지게 된다. 이를 보안하기 위해 패리티 보존형 가역 논리게이트(Parity-Preserving Reversible logic gate)[9]가 소개되었다. 이를 이용하여 다양한 패리티 보존형 가역 논리게이트가 소개되었다. 그러나 기존의 패리티 보존형 가역 논리게이트의 경우 단독으로 논리 회로를 구성할 수 없기 때문에 여러 개의 패리티 보존형 가역 논리게이트를 이용하여 가역논리 게이트의 기본 역할을 하는 Toffoli Gate(TG)를 패리티 보존형 TG로 구성하여 사용한다.

2006년 IEEE TIM 저널에서 가역 논리게이트 2개를 이용하여 패리티를 보존하는 Testable block[12]이 소개되었다. 이는 Testable block만을 이용하여 논리 회로를 모두 구성할 수 있다는 장점을 가진다.

본 논문에서는 오류 주입을 확인이 가능한 새로운 패리티 보존 가역 논리 게이트를 제안한다. 본 논문에서 제안하는 패리티 보존형 가역 논리게이트의 경우 기존의 패리티 보존형 가역 논리게이트가 단독으로 논리 회로를 구성할 수 없다는 단점을 역시 보안하는 패리티 보존형 가역 논리게이트이다. 제안하는 패리티 보존형 가역 논리게이트를 사용하여 논리 회로를 구성하였을 경우 기존의 testable block으로 논리 회로를 구성하거나 패리티 보존형 TG로 논리 회로를 구성하였을 경우 보다 효율적으로 사용 할 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 기존의 패리티 보존형 가역 논리게이트를 설명하고, 본 논문에서 제안하는 패리티 보존형 가역 논리게이트와 비교대상이 될 testable block을 소개한다. Ⅲ장에서 논문에서 제안하는 새로운 패리티 보존형 가역 논리게이트를 소개한다. 논리 게이트를 소개하고, 기존 방법들과 비교 결과를 소개한다. 마지막으로 Ⅳ장에서 결론을 맺는다.

Ⅱ. 기존의 패리티 보존형 가역 논리 게이트 Parity-Preserving Reversible Logic Gate (PPRLG)

본 장에서는 패리티 보존형 가역 논리게이트(Parity-Preserving Reversible logic gate, PPRLG)를 정의한다. 용어정의와 기존 오류 주입을 확인하는 가역 논리게이트를 소개한다.

1. 용어 정의

본 절에서는 기존의 오류 주입을 확인하는 가역 논리게이트에 대한 설명 전에 본 논문에서 사용하는 용어에 대한 정의를 한다.

정의 1. [가역 논리게이트, Reversible logic gate (RLG)]

입력 값과 출력 값의 개수가 같고, 입력/출력 어느 쪽에서도 서로 검색이 가능한 게이트를 가역 논리 게이트(Reversible logic gate, RLG)라고 한다.

고전적인 논리 게이트와 RLG를 비교하면 그림 1, 표 1과 같다. 고전적인 논리게이트의 경우에는 출력 값(Q=1 혹은 0)으로는 입력 값을 결정 할 수 없다. 하지만, RLG의 경우 출력 값의 쌍 (P,Q)를 이용하여 입력 값을 결정할 수 있게 된다. 대표적인 RLG는 Feynam Gate(FG)[7], Toffoli Gate(TG)[5], Fredkin Gate(FRG)[6], New Gate(NG)[8], Feynam Double Gate(F2G)[9]가 있다.

TG는 고전적인 가역 계산 (classical reversible computation) 이론에서 가장 기본적인 역할을 하는 게이트이다. TG는 논리적으로 잘 알고 있는 AND 게이트의 역할을 하기 때문이다. 실제로 모든 고전적인 논리

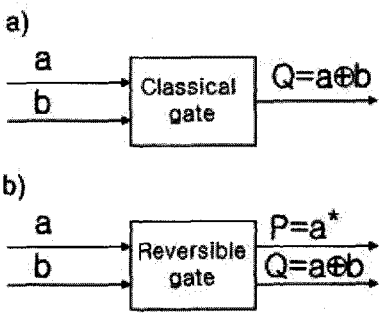


그림 1. a) 고전적인 XOR게이트, b) 가역논리 XOR게이트
Fig. 1. a) Classical XOR gate, b) reversible XOR gate.

표 1. (a) 고전적인 XOR 게이트 진리표,
(b) 가역 논리 XOR 게이트의 진리표
Table 1. (a) Truth table of the classical XOR gate,
(b) Truth table of reversible XOR gate.

(a) 고전적인 XOR 게이트

a	b	Q
0	0	0
0	1	1
1	0	1
1	1	0

(b) 가역 논리 XOR 게이트

a	b	P	Q
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

회로는 AND 게이트들만의 조합으로 만들 수 있으며, 가역 계산의 논리 회로도 마찬가지로 TG들만의 조합으로 만들 수 있다.

정의 2. [패리티 보존형 논리게이트, Parity-preserving logic gate (PPLG)]

입력 값 $I_v=(A,B,C)$, 출력 값 $O_v=(P,Q,R)$일 경우 $A\oplus B\oplus C=P\oplus Q\oplus R$을 만족 한다. 즉, 입력 값과 출력 값의 패리티가 같은 경우를 패리티 보존형 논리 게이트라(PPLG)고 한다.

정의 3 .[패리티 보존형 가역 논리게이트, Parity-preserving reversible logic gate (PPRLG)]

정의 2와 정의 3을 동시에 만족하는 경우를 패리티 보존형 가역 논리게이트(PPRLG)이다.

정의 4. [Garbage-output]

Garbage-output은 현재 RLG의 출력 값이 다른 RLG의 입력 값으로 사용 되지 않는 것을 의미한다. 그림 1에서 '*'가 가역 논리 XOR게이트의 Garbage-output을 의미한다. RLG에서는 Garbage-output 수가 적을수록 안전하고, 효율적인 게이트이다[13]. 본 논문에서 이 후 가역 논리게이트에서는 따로 garbage-output를 표시하지 않는다.

RLG 중에서 정의 3을 만족하는 대표적인 PPRLG로는 그림 2와 같이 F2G와 FRG가 있다.

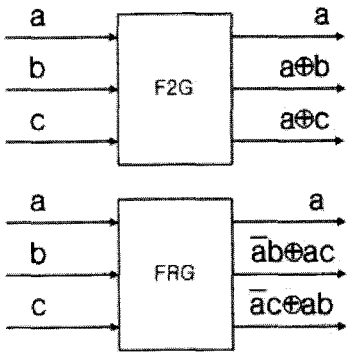


그림 2. 대표적인 PPRLGs
Fig. 2. Commonly used PPRLGs.

2. 기존의 오류 주입을 확인하는 가역 논리게이트

1절에서 소개한 PPRLGs의 F2G와 FRG는 패리티를 유지하면서 오류 주입을 확인 할 수 있는 기능은 가지고 있지만, TG와 동일하게 F2G와 FRG의 단독 조합으로 모든 가역 논리 회로를 구성할 수 없다. 따라서 F2G와 FRG를 이용하여 패리티 보존형 TG[9]를 만들어서 논리 회로에 사용하게 된다.

RLG TG를 PPRLG로 표현할 경우 그림 3과 같이 2개의 F2G와 1개의 FRG로 표현 될 수 있다[6]. F2G와

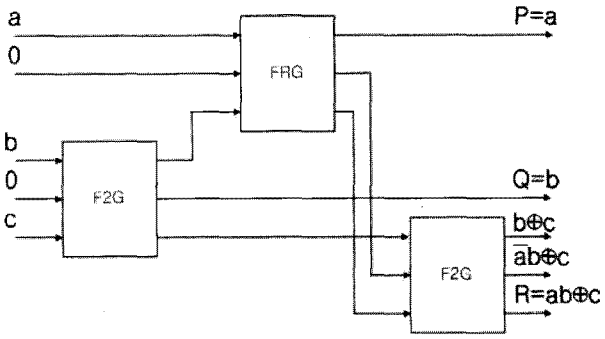


그림 3. F2G[9], FRG[6] 의 Parity-preservation TG gate
Fig. 3. TG with parity-preservation using F2G[9], FRG[6].

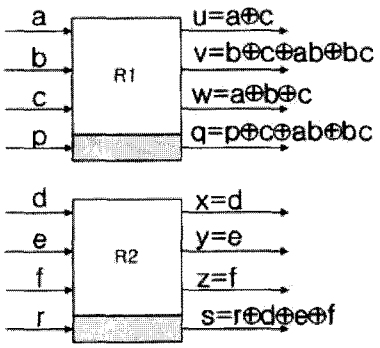


그림 4. 가역 논리 게이트 R1, R2
Fig. 4. Reversible-logic gate R1 and R2.

FRG로 구성 된 패리티 보존형 TG 게이트는 6개의 XOR연산, 3개의 AND연산 그리고 2개의 NOT연산의 단위 연산으로 구성되고, 3-클럭 사이클의 시간이 요구된다. 또한 2개의 Garbage-output과 5개의 입력 값을 가진다.

2006년 Dilip P. Vasudevan[12] 등이 두 개의 RLG (R1, R2)를 이용하여 오류 주입을 확인할 수 있는 testable block을 소개하였다. 그림 4는 RLG인 R1과 R2이고, 이를 이용하여 그림 5와 같이 testable block을 구성한다.

Testable block에서 R1 혹은 R2에 오류가 발생하지 않았다면 출력 값 q,s는 서로 보수의 관계를 가지게 된다. 즉, $q=1$이면 $s=0$이다.

각 RLG의 단위 연산량을 살펴보면 R1의 경우 2개의 AND, 6개의 XOR 연산량이고, R2의 경우 3개의 XOR 연산으로 구성된다.

R1를 이용하여 boolean 함수 중 OR, XOR 게이트, NAND와 XNOR 게이트를 구성하면 그림 6과 같다.

Testable block를 이용하여 boolean 함수를 구성하였을 경우의 연산량은 다음과 같다. 이 때 A는 AND 연산, X는 XOR 연산을 말한다.

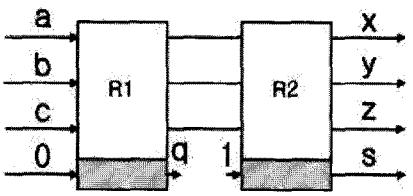


그림 5. Testable block
Fig. 5. Testable block.

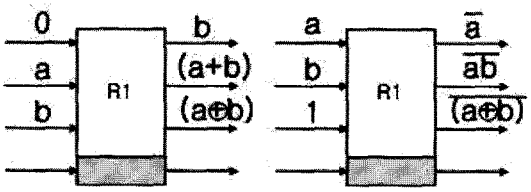


그림 6. R1 게이트로 구성 된 Boolean 함수
Fig. 6. Boolean Function using R1 gate.

표 2. Testable block을 이용한 boolean 함수의 연산량
Table 2. Complexity of boolean function using testable block.

Boolean 함수	연산량
OR, XOR, NOT XNOR, NAND	$2A+9X$
NOR, AND	$4A+15X$

Ⅲ. 제안하는 패리티 보존형 가역 논리 게이트 (Parity-Preserving Reversible Logic Gate, PPRLG)

3-입력, 3-출력 값을 가지는 새로운 패리티 보존형 가역 논리 게이트는 다음과 같다.

정리 1. [제안하는 PPRLG : SKG]

3-입력, 3-출력인 SK gate(SKG)는 그림 7과 같이 $I_v=(a,b,c), O_v=(ab\oplus\bar{b}c, a\bar{b}\oplus bc, b)$로 정의되고, 이는 PPRLG를 만족한다. 이 때, I_v는 입력 벡터, O_v는 출력 벡터이다.

Proof. PPRLG를 만족하기 위해서는 RLG를 만족해야하며 패리티 보존형이어야 한다. 먼저, RLG는 표 3에서 확인할 수 있다. 표 3은 SKG의 진리표이다. 입력 수와 출력 수가 같고, 입력과 출력이 일대일 대응이다.

패리티 보존형은 다음 식을 통하여 만족함을 알 수 있다.

$$P\oplus Q\oplus R=(ab\oplus\bar{b}c)\oplus(a\bar{b}\oplus bc)\oplus b=a\oplus b\oplus c.$$

따라서 제안하는 SKG는 PPRLG임을 알 수 있다. □

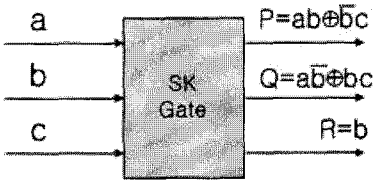


그림 7. 제안하는 PPRLG
Fig. 7. Proposed PPRLG.

표 3. 제안하는 SK 게이트 진리표
Table 3. Truth table of the proposed SK gate.

a	b	c	P	Q	R
0	0	0	0	0	0
0	0	1	1	0	0
0	1	0	0	0	1
0	1	1	0	1	1
1	0	0	0	1	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

표 4. 패리티 보존형 TG와 SKG를 이용한 boolean 함수 비교
Table 4. Comparative of boolean function using parity-preserving TG and SKG.

	Boolean 함수	연산량	Garbage-output	RLG 개수	clock cycle	input constant
[9]	XOR, AND, NOT, OR	$6X+3A+2N$	4	3	3	5
	XNOR, NAND, NOR	$12X+6A+4N$	7	6	6	8
[12]	OR, XOR, NOT, XNOR, NAND	$8X+2A$	3	2	2	5
	NOR, AND	$13X+4A$	6	3	4	8
SKG	XOR, XNOR, NAND, NOR	$4X+8A+2N$	3	2	2	4
	AND, OR, NOT	$2X+4A+1N$	2	1	1	3

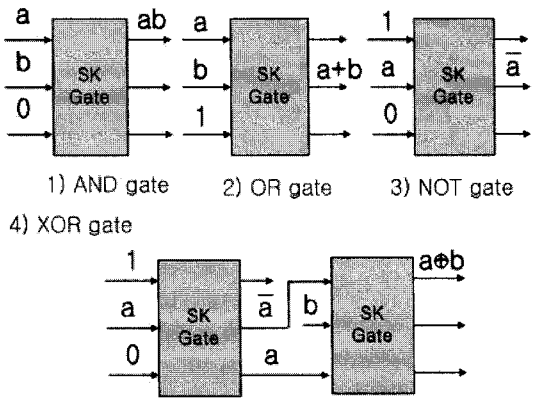


그림 8. SK 게이트로 표현된 Boolean Function
Fig. 8. Boolean Function using SK gate.

제안하는 PPRLG인 SKG의 단위연산은 2번의 XOR연산과 4번의 AND, 1번의 NOT연산으로 구성되며, 그림 8과 같이 모든 boolean 함수를 구성 할 수 있다.

표 5는 SKG를 이용하여 boolean 함수를 구성하였을 경우에 요구하는 연산량과 [9], [12]의 결과를 비교한 것이다. A는 AND 연산, X는 XOR 연산 그리고 N은 NOT 연산을 의미한다. 표 5에서 볼 수 있듯이 패리티 보존형 TG를 이용한 [9] 논문과 비교하였을 경우 하드웨어 연산량에서는 크게 차이를 보이지 않지만, Garbage-output 개수, RLG의 개수, 클럭 사이클 그리고 input constant에서 효율적임을 알 수 있다. 그리고 [12]논문에서 제안한 testable block을 이용할 경우와 비교하였을 경우 보다 효율적임을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 효율적인 오류 주입을 확인할 수 있는 가역 논리 게이트인 패리티 보존형 가역 논리 게이트를 새롭게 제안한다. 제안하는 패리티 보존형 가역 논리게이트는 기존의 패리티 보존형 가역 논리게이트와는 달리 단독으로 논리 연산을 구성할 수 있으며, 기존에 존재하는 가역 게이트에서 사용되는 논리적 연산량이 적기 때문에 boolean 함수 등 논리 연산을 효율적으로 구성할 수 있다.

참 고 문 헌

[1] Landauer. R, "Irreversible and Heat Generation in the Computation Process", IBM Journal of research and development, 5, pp183-191, 1961.
[2] Schrom. G, "Ultra Low Power CMOS Technology", PhD Thesis, Technician Universitat Wien, 1998.
[3] M. Nielsen and I. Chaung, "Quantum Computation and quantum Information", Cambridge University Press, 2000.
[4] Merkle. R. C, "Two Types of Mechanical Reversible Logic", Nanotechnology pp114-131, 1993.
[5] T. Toffoli, "Reversible Computing," Tech memo MIT/LCS/TM-151, MIT Lab for Comp. Sci, 1980.
[6] E. Fredkin and T. Toffoli, "Conservative logic," Int'l J. Theoretical Physics, Vol. 21, pp. 219 -

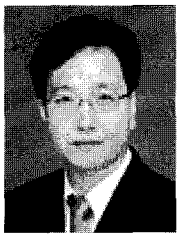
253, 1982.
[7] R. Feynman, "Quantum Mechanical Computers," Optics News, Vol. 11, pp. 11 - 20, 1985.
[8] Azad Khan Md. M. H. "Design of full adder with reversible gate". International Conference on Computer and Information Technology, Dhaka, Bangladesh, pp. 515-519, 2002.
[9] Parhami B. "Fault tolerant reversible circuits", Proc. 40th Asilomar Conf. Signals, Systems, and Computers, October 2006, Pacific Grove, CA, pp.1726-1729, 2006.
[10] B. Parhami, "Parity-preserving Transformations in Computer Arithmetic," Proc. SPIE Conf. Advanced Signal Processing Algorithms, Architectures, and Implementations XII, pp. 403-411, 2002.
[11] B. Parhami, "An Approach to the Design of Parity-Checked Arithmetic Circuits," Proc. 36th Asilomar Conf. Signals, Systems, and Computers, pp. 1084-1088, 2002.
[12] Dilip P. Vasudevan, Parag K. Lala, Fia Di and Patrick Parkerson, "Reversible-Logic Design With Online Testability", IEEE Transactions on instrumentation and measurement, Vol.55, No. 2, 2006.
[13] Thapliyal, H. and M.B. Srinicas, "Novel reversible TSG gate and its application for designing reversible carry look ahead adder and other adder architectures", ACSAC'05, LNCS 3740, pp.775-786, 2005.

저 자 소 개

김 성 경(학생회원)
2005년 2월 동의대학교 수학과 학사
2005년 3월~2007년 8월 고려대학교 정보경영공학전문대학원 석사과정
2007년 8월~현재 고려대학교 정보경영공학전문대학원 박사과정
<주관심분야: 부채널 공격, 공개키 암호, 암호칩 설계 기술>

김 태 현(학생회원)
2002년 2월 서울시립대학교 수학과 학사
2004년 8월 고려대학교 정보보호대학원 석사
2009년 2월 고려대학교 정보경영공학전문대학원 박사
2006년 4월 일본 Future Unuversity-Hakodate, 방문연구원
2009년 8월~현재 한국전자통신연구원(ETRI) 부설연구소 연구원
<주관심분야: 공개키 암호, 부채널 공격, 암호칩 설계 기술>

한 동 국(정회원)
1999년 2월 고려대학교 수학과 학사
2002년 2월 고려대학교 수학과 이학석사
2005년 2월 고려대학교 정보보호대학원 공학박사
2004년 4월~2005년 4월: 일본 Kyushu Univ., 방문연구원
2005년 4월~2006년 4월: 일본 Future Univ.-Hakodate, Post.Doc.
2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재: 국민대학교 수학과 조교수
<주관심분야: 암호시스템 안전성 분석 및 고속 구현, 부채널 분석, RFID/USN 정보보호 기술>



홍 석 희(정회원)
1995년 2월 고려대학교 수학과 학사
1997년 2월 고려대학교 수학과 이학석사
2001년 2월 고려대학교 수학과 이학박사
1999년 8월~2004년 2월 (주)시큐리티 테크놀로지스 선임연구원
2003년 3월~2004년 2월 고려대학교 시간강사
2004년 4월~2005년 2월 K.U. Leuven 박사후 연구원
2005년 3월~2008년 8월 고려대학교 정보경영공학전문대학원 조교수
2008년 9월~현재 고려대학교 정보경영공학전문대학원 부교수
<주관심분야: 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 포렌식>