Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.603

확장성을 고려한 다수결 게이트 기반의 QCA 4-to-2 인코더 설계*

김 태 환,† 전 준 철‡
국립금오공과대학교 컴퓨터 공학과

Design of Extendable QCA 4-to-2 Encoder Based on Majority Gate*

Tae-Hwan Kim,† Jun-Cheol Jeon‡
Computer Engineering at Kumoh National Institute of Technology

요 약

인코딩은 정보의 형태나 형식을 표준화, 보안, 처리 속도 향상, 저장 공간 절약 등을 위해 다른 형태나 형식으로 변환 또는 처리 하는 것을 말한다. 정보 통신에서 송신자의 정보가 다른 형태로 수신자에게 전달할 수 있도록 정보를 변환하는 것도 인코딩이다. 이 처리를 수행 하는 장치를 인코더라 부른다. 본 논문에서는 양자 컴퓨터에서 요구되는 인코더 중 가장 기본적인 4-to-2 인코더를 제안한다. 제안한 인코더는 2개의 OR 게이트를 사용하여 구성된다. 제안한 구조는 셀의 간격을 최적화 하고 배선간의 잡음을 최소화하는 것을 목적으로 설계한다. 제안된 인코더를 QCADesigner를 통해 시뮬레이션을 수행하고, 그 결과를 분석하여 효율성을 확인한다.

ABSTRACT

Encoding means converting or processing form or format of information into the other forms to standardize, secure, improve processing speed, store saving spaces and etc. Also, Encoding is converting the information so as to do transmit other form on the sender's information to the receiver in Information-Communication. The device that is conducting the processing is called the encoder. In this dissertation, proposes an encoder of the most basic 4-to-2 encoder. proposed encoder consists of two OR-gate and the proposed structure designs and optimize the spacing of the cell for the purpose of minimizing noise between wiring. Through QCADesigner conducts simulation of the proposed encoder and analyzes the results confirm the effectiveness.

Keywords: Quantum-dot Cellular Automata, Circuit Design, Quantum Computer, Encoder

I. 서 론

정보 통신 기술의 발전은 수많은 분야의 산업 정보화를 이끌었고, 이는 급속한 경제적, 사회적 발전을 이루는 토대가 되었다. 하지만 이러한 정보를 악용하여 불법적인 이득을 취하려는 시도 또한 수없이 많이 존재 하였고, 이를 막기 위한 보안 기술 또한 함께 발전하였다[1].

하지만 CMOS 집약성의 한계가 다가오면서 기존의 암호체제로는 더 이상 보안성을 유지 할 수가 없게 되었다.

공개키 암호체계의 근간을 이루는 건 소인수 분해

Received(04. 01. 2016), Modified(05. 19. 2016), Accepted(05. 19. 2016)
* 이 논문은 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2015R1A2A1A15055749).
* 본 논문은 2015년도 동계 학술 대회에 발표한 우수논문을 개선 및 확장한 것임
† 주저자, kth4462@gmail.com
‡ 교신저자, jcjeon@kumoh.ac.kr(Corresponding author)

이다. 기존 컴퓨터는 N자리 수를 소인수 분해 하는데 걸리는 시간은 $\exp[(\ln N)^{1/3}(\ln(\ln N)^{2/3})]$에 비례하지만 Shor의 양자 풀이법을[2] 사용하면 약 $\ln N^3$ 보다 적은 시간이 걸린다. 이 알고리즘의 핵심은 양자의 중첩이라는 성질을 이용하여 모든 연산을 병렬적 또는 동시에 처리함으로서 빠르게 결과에 도달 할 수 있다는 것이다. 양자 컴퓨터는 기존 컴퓨터와는 차원이 다른 속도로 현대암호를 모두 깰 수 있는 잠재력을 가진 양자 컴퓨터는 전 세계적으로 주목을 받기 시작했다[3].

양자 컴퓨터에 사용된 양자점 셀룰라 오토마타(Quantum-dot cellular automata, QCA)는 CMOS 집약성의 한계점을 극복할 수 있는 새로운 대체 기술이다. QCA는 양자 역학에 기반을 두기 때문에 분자 수준의 아주 작은 크기인 나노크기(nano-scale)에서 하드웨어 설계를 수행하고, 기존의 디지털 논리회로 보다 더 빠른 연산을 수행하며, 소비되는 전력이 매우 작은 것이 특징이다[4].

1993년 Lent등에 의해 처음으로 소개된 QCA는 셀의 기본 동작을 사용하여 간단한 회로들을 구현했다. 이후 전가산기, 인코더와 같은 조합 논리회로부터 산술 논리회로, 레지스터 등을 이용한 대규모의 VLSI 회로의 설계까지 다양하게 제안되었다[5].

본 논문에서는 양자 컴퓨터에서 요구되는 인코더 중 가장 기본적인 4-to-2 인코더를 제안한다. 인코더의 여러 기능중 제안하는 인코더는 2n 비트가 입력되면 출력의 n비트 중 선택적으로 신호가 출력되는 구조이다. 기존에 QCA상에서 제안된 인코더의 문제점을 살펴보고 제안하는 인코더와 비교, 분석해 본다. 기존의 디지털 논리회로 상에서 인코더의 논리회로도는 Fig. 1.과 같다.

이는 4개의 입력과 2개의 출력을 가지는 구조로서 Fig. 1.의 인코더에서 입력 D0, D1, D2, D3 에 차례대로 1이 들어오면 출력 A, B는 차례대로 00, 01, 10, 11이 나온다. 이 구조는 4개의 입력 중 어느 한 입력으로만 들어오는 경우를 제외한 나머지 경우는 발생하지 않는다고 가정하여 설계된 것이다.

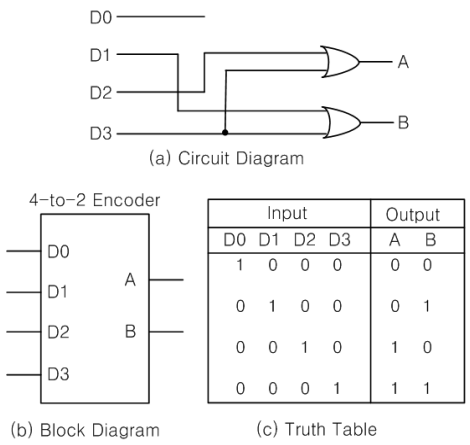
II. QCA 기본 개념

셀은 네 개의 양자 점으로 구성되어 있다. Fig. 2.(a)와 같이 셀은 양자 점들 간에 터널링(tenneling) 할 수 있는 두 개의 과도(transition) 전자를 가지고 있다.

쿨롱 반발력 때문에 이 과도 전자는 항상 대각선 방향 반대쪽에 위치한다. 에너지가 등가인 두 가지의 편극(polarization) 형태가 존재하며 +1(1), -1(0)으로 나타낸다[5].

Fig. 2.(b)와 같이 45° 회전된 셀의 표현과 Fig. 2.(c).와 같이 이진 배선에서의 신호의 전파를 나타내고 있다. 표준 셀은 신호가 입력되면 인접된 셀 간에 전자들의 쿨롱 반발력에 의해 같은 편극의 상태로 전파된다. 그러나 45° 회전된 셀의 경우 인접한 셀과 반대의 편극을 가진다.

배선의 교차는 Fig. 3.과 같이 표준 셀과 45° 회전된 셀을 이용하여 수행한다. 표준 셀과 45° 회전된 셀에 대한 두 개의 배선은 서로 영향을 주지 않고 신



Input				Output	
D0	D1	D2	D3	A	B
1	0	0	0	0	0
0	1	0	0	0	1
0	0	1	0	1	0
0	0	0	1	1	1

Fig. 1. 4-to-2 Encoder

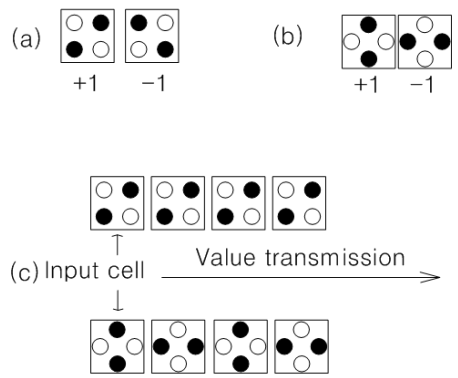


Fig. 2. QCA Wiring : (a) Two kind of cell state, (b) 45° rotating cell, (c) Standard wiring and 45° rotating wiring

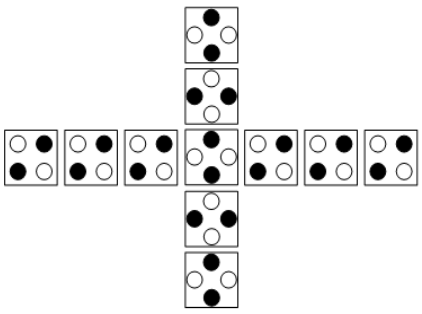


Fig. 3. The intersection of standard cell and 45° rotating cell

호의 흐름을 올바르게 전달하는 설계 구조이다. QCA 상에서 존재하는 논리 게이트는 Fig. 4.와 같이 다수결 게이트와 인버터가 존재한다. Fig. 4.(a)는 다수결 게이트를 나타낸다. 이 게이트는 3개의 입력 셀 A, B, C와 1개의 출력 셀 F를 가지고 있다. 다수결 게이트는 입력 셀들의 편극에 따라서 중앙에 있는 셀의 편극이 결정되고, 그 편극이 출력 F에 영향을 주게 되어 신호가 전파된다. 인버터는 Fig. 4.(b)와 같이 입력 신호와 출력 신호의 편극이 반대되어 신호가 전파된다.

Fig. 4.(c)는 제안한 인코더에 사용된 45° 회전된 배선과 표준 배선을 사용한 인버터이다. 이 인버터를 사용하는 이유는 교차부에서 셀들이 서로에게 영향을 최소화 하고 값의 진행 방향과 상태를 유지하기 위함이다. 45° 회전된 세로 셀에서 값이 전달될 때 표준 배선을 수직으로 연결하면 한 셀 차이로 인

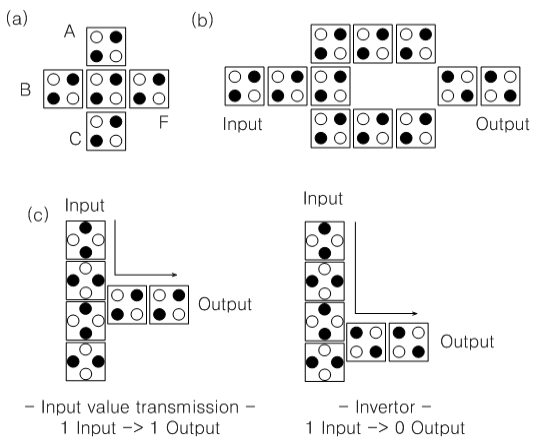


Fig. 4. (a) Majority gate, (b) Invertor, (c) Using a standard wiring and 45° rotating wiring invertor

버터를 설계 할 수 있다.

또 논리 회로에서 사용되는 클록(Clock)이라는 개념을 QCA에서도 동일하게 사용된다. 클록이란 디지털 회로에서 클록 신호에 맞추어 신호의 처리를 하는 동기 처리를 하기 위한 논리상태 H(high, 1), L(low, 0)이 주기적으로 나타나는 주파수를 의미한다.

Fig. 5.에서 보면 클록 레벨이 상승 하거나 하강할 때 데이터 값의 변화가 생긴다. 이를 엣지 트리거(Edge Trigger)라고 하고 상승 엣지, 하강 엣지 두 가지 경우가 있다.

Fig. 6.를 보면 엣지 트리거와 달리 클록 레벨이 상승 또는 하강 후 다음 변화가 있기 전까지 범위 동안 데이터 변화가 생기는 것을 레벨 트리거(Level Trigger)라고 한다.

본 논문에서는 QCA 인코더 설계 과정에서도 신호의 동기화를 위해 클록 0에서 클록 3까지 4개의 클록을 사용 할 것이다.

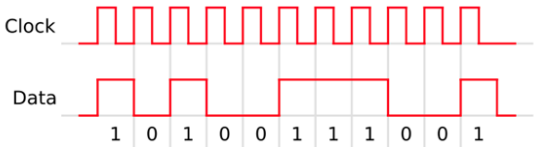


Fig. 5. Clock example 1

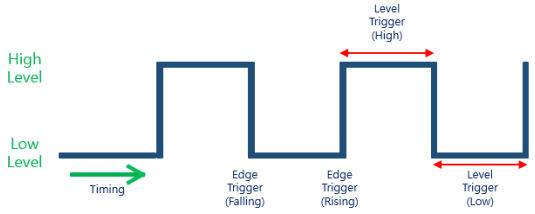


Fig. 6. Clock example 2

III. 확장성을 고려한 인코더 설계 및 분석

입력 신호를 일정한 규칙에 따라 정해진 값만 출력하는 인코딩 과정은 같은 입력 값이라면 같은 출력 값이 나와야 한다. 본 논문에서 제안 하는 4-to-2 인코더는 4개의 입력이 들어오면 2개의 출력으로 4가지 경우의 수를 나타내어 준다.

3.1 우선 순위 인코더

Fig. 7.은 우선순위 인코더를 QCA로 설계를 한 인코더이다[6]. 우선순위 인코더란 기본 인코더에 우선순위를 도입한 것으로, 여러 신호 중 우선순위가 높은 순으로 출력되는 인코더를 말한다. Fig. 8.에서 보는 시뮬레이션 결과는 기본 4-to-2 인코더의 출력만 보여주고 D0~D3까지 출력 단자의 클록이 0 이기 때문에 클록 0 사이클에 따라 엣지 트리거로 값이 변화한다.

이 인코더(Fig. 7.)는 설계 공간에 비해 셀들의 밀집도가 높다. 그 결과 간섭이 생겨 편극 값이 일정하지 않았다. 또한 입력 부분과 출력 부분의 위치가 분리되어 있지 않아 확장성에 대한 문제도 있다. 현재 8-to-3 인코더로 확장을 하려면 전체적인 형태가 완전히 바뀌게 설계가 된다. 또한 D2 입력부분은 Fig. 9.에서 보는 것처럼 3차원으로 쌓아올린 형태로 설계가 되어 실제 하드웨어 설계에서 문제가 될 수 있다[6].

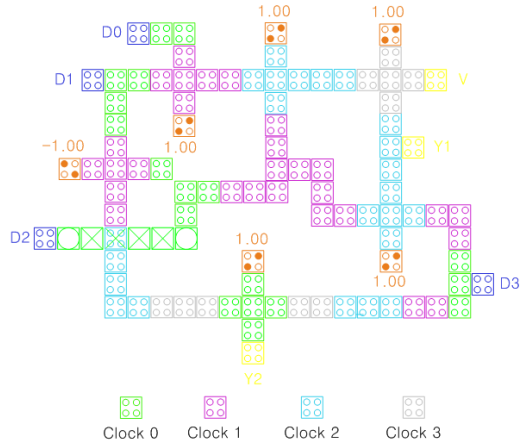


Fig. 7. Priority encoder

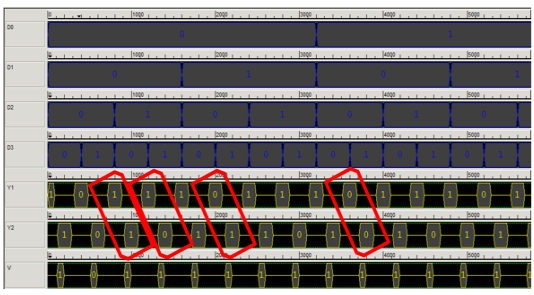


Fig. 8. Simulation results of Priority Encoder

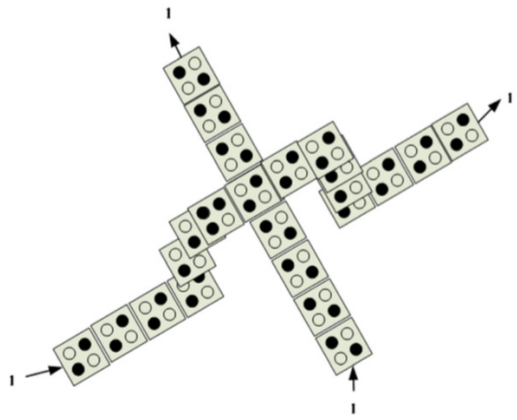


Fig. 9. 3D Design of the QCA

3.2 확장성을 고려하지 않고 설계한 인코더

Fig. 10.은 기존의 우선순위 인코더(Fig. 7.)을 참고하여 확장성과 편의성을 고려하지 않고 설계한 인코더이다. 이 인코더의 시뮬레이션 결과(Fig. 11.)를 보면 출력해주는 값은 기존의 우선순위 인코

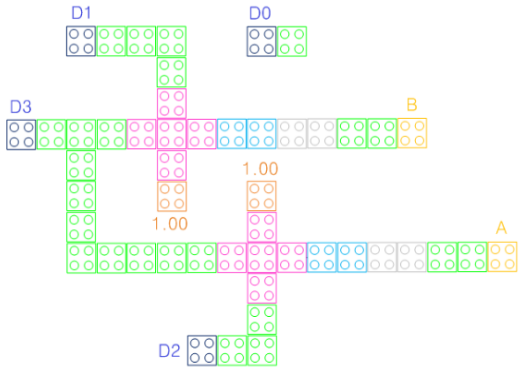


Fig. 10. 4-to-2 encoder

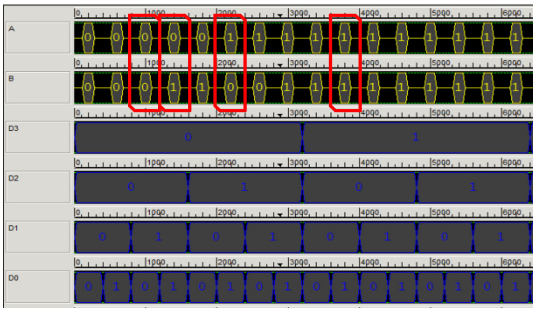


Fig. 11. Simulation results of the encoder

더와 제안하는 인코더와 동일하게 출력된다. 하지만 여전히 입력부의 위치가 일정하지 않아 불규칙한 모습을 보여주고 있고 D0 부분은 다른 회로들과 완전히 분리되어 있는 모습을 볼 수 있다. 따라서 이 4-to-2 인코더는 단일 인코더로서의 기능은 수행 가능 하지만 8-to-3 인코더로 확장하거나 다른 회로들과의 호환은 기대하기 힘들다.

3.3 제안하는 인코더

제안하는 인코더는 Fig. 12.와 같다. 인코더의 기본 회로도를 참고하였다(Fig. 1.). Fig. 13.에서 시뮬레이션 결과를 보면 기존의 인코더들과 동일한 기능을 구현한 것을 확인 할 수 있다. 확장성을 고려하여 입력 부분은 좌측 상단, 출력 부분은 우측으로 분리 하였고, 논리 게이트로 OR 게이트 2개만 사용하여 설계를 하였다. 그 결과로 간섭을 최소화 시켰고 확장성이 증가되었다.

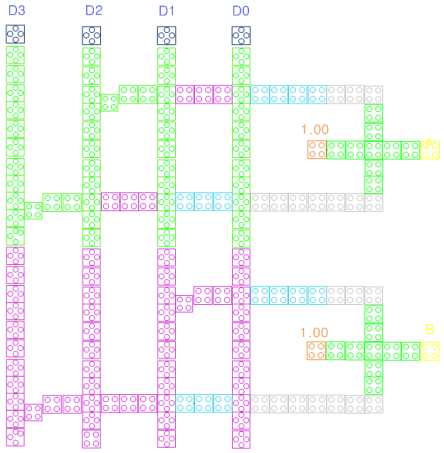


Fig. 12. The proposed encoder

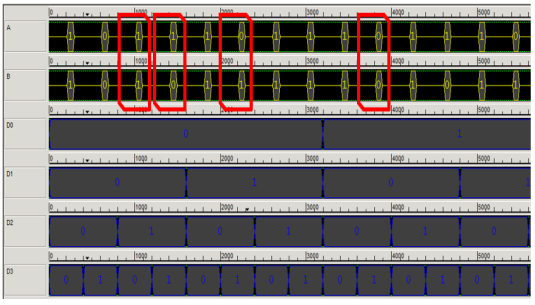


Fig. 13. Simulation results of the proposed encoder

3.4 비교 분석

Table 1.에서 보면 기존 우선순위 인코더의 결과 값은 회로 내부에서 값이 전달되면서 간섭이 일어나 편극 편차가 생긴다. 그에 비해 제안한 인코더의 결과 값은 간섭이 일어나지 않아 편극 범위가 일정하게 유지되는 것을 확인 할 수 있다. 제안한 인코더가 기존의 인코더 보다 사용된 셀 수가 많지만 단위 면적당 셀 비율과 사용된 게이트 수 그리고 클록은 동일하게 사용된 것을 확인 할 수 있다.

Table 2.를 보면 사용된 셀 수, 단위 면적당 셀 비율, 편극 등 기본 인코더가 좋게 나타나는 것처럼 보이지만 다양한 논리게이트들이 연결되어 동작하는 디지털 회로의 특성한 단일 인코더로 사용되는 경우는 거의 없기 때문에 확장성과 호환성이 좋은 제안한

Table 1. Compare the priority encoder and proposed encoder

	priority encoder	proposed encoder
Number of cell	98 cell	165 cell
Number of clock	5 clock	5 clock
cell ratio	32.6%	32.6%
polarization	$-8.73 \sim 9.54e$	$\pm 9.54e$
Number of gate	2	2
I/O Connector division	not division	division
Scalability	Bad	Good

Table 2. Compare the basic encoder and proposed encoder

	priority encoder	proposed encoder
Number of cell	49 cell	165 cell
Number of clock	5 clock	5 clock
cell ratio	17%	32.6%
polarization	$\pm 9.54e$	$\pm 9.54e$
Number of gate	2	2
I/O Connector division	not division	division
Scalability	Bad	Good

인코더가 더 유용하게 사용 될 수 있다.

비슷한 설계 조건으로 볼 수 있지만 제안한 인코더는 입출력 단자가 분리되어 있어서 확장하기에 용이하다.

IV. 결 론

양자 컴퓨터의 효과적인 구현을 위해 QCA상에서 많은 논리회로들이 설계되고 있다. 본 논문에서는 하드웨어 설계에서 필수적인 조합 논리회로인 인코더를 설계하였다. 설계된 회로는 QCADesigner를 사용하여 시뮬레이션 하였고, 기존에 설계된 인코더와 비교 및 분석을 하였다. 기존 CMOS상의 컴퓨터와는 비교 할 수 없을 정도의 빠른 속도로 기존 암호 체제를 위협하는 양자 컴퓨터인 만큼 가장 기본이 되는 논리 회로들의 설계가 중요하다. 제안한 인코더는 입출력 단자 위치의 분리와 결과 값의 일정함으로 안정성과 확장성을 확인하였다.

References

[1] Hae-Sin Go, Gyeong-Cheon Im, Gi-Woong Kim, Chang-Ho Kim and Jun-Gu Lee, "Quantum Encryption -Key Distribution Security Analysis according to The Quantum State Change," The Journal of The Korean Institute of Communication Sciences 31(9), pp. 70-76, Aug. 2014.

[2] P. Shor, " Polynomial-Time Algorithm for Prime Factorization and Discrete Logarithms on a Quantum Computer," Proceedings of the 35th Annu. Symp. on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, California, pp.124-134. Nov. 1994.

[3] Sun-Chill Lee, "Public Key Crypt- ography and Shor Algorithm," Korea Institute of Information Security And Cryptology pp. 1-2, Jun. 2004.

[4] C. S. Lent, P. D Tougaw, W. Porod and G. H. Bernstein, "Quantum Cellular Aautomata," Nano technology, vol. 4, no 1, pp. 49-57, Jan. 1993.

[5] C. S. Lent and P. D Tougaw, "A Device Architecture for Computing with Quantum Dots," Proceedings of the IEEE, vol. 85, no. 4, pp. 541-557, Apr. 1997.

[6] B. Ghosh, S. Gupta, S. Kumari and A. Salimath, "Novel Design of Combinational and Sequential Logical Structures in Quantum Dot Cellular Automata" Journal Of Nanostructure in Chemistry, vol. 3, no 15, pp 3-8, Dec. 2013.

〈저 자 소 개〉

김 태 환 (Tae-Hwan Kim) 학생회원
2015년 3월~현재: 금오공과대학교 컴퓨터공학 전공
〈관심분야〉 암호학, 암호회로설계, 양자 암호 등

전 준 철 (Jun-Cheol Jeon) 종신회원
2000년 2월: 금오공과대학교 컴퓨터공학과 졸업
2003년 2월: 경북대학교 컴퓨터공학과 석사
2007년 2월: 경북대학교 컴퓨터공학과 박사
2012년 9월~현재: 금오공과대학교 컴퓨터공학과 교수
〈관심분야〉 암호학, 암호회로설계, 암호프로토콜설계, 양자암호