Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 3 pp. 1147-1152, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.3.1147

디지털 하드웨어 난수 발생기에서 출력열 특성 처리 분석

홍진근[1*]
[1]백석대학교 정보통신학부

Analysis of Output Stream Characteristics Processing in Digital Hardware Random Number Generator

Jin-Keun Hong[1*]
[1]**Division of Information Communication, Baekseok University**

요 약 본 논문은 의학 분야에서 사용되는 하드웨어 발생기 디지털 난수 출력열의 특성 처리 분석을 주요 이슈로 한다. 하드웨어 이진 난수를 기반으로 하는 난수발생기의 출력열은 지연, 지터, 온도 등의 요소로부터 영향을 받는다. 본 논문에서는 하드웨어 출력 난수열에 영향을 주는 주요 요소에 대해 살펴보고, 출력열과 암호알고리즘, 부호알고리즘이 결합된 출력열의 난수성을 분석하였다. 분석된 결과는 난수성 주요 검증 항목에 의해 평가되었다.

Abstract In this paper, it is key issue about analysis of characteristics processing of digital random output stream of hardware random number generator, which is applied in medical area. The output stream of random number generator based on hardware binary random number is effected from factors such as delay, jitter, temperature, and so on. In this paper, it presents about major factor, which effects hardware output random number stream, and the randomness of output stream data, which are combined output stream and postprocessing data such as encryption algorithm, encoding algorithm, is analyzed. the analyzed results are evaluated by major test items of randomness.

Key words : Noise, Random, Security level

1. 서론

난수열을 생성하는 실난수 발생기는 통계적인 랜덤성(randomness)을 제공하는 것이 핵심이며, 일반적으로 자연현상으로부터 추출 가능한 비예측적이고 모조할 수 없는 비결정적인 잡음원을 사용한다. 의사난수발생기의 경우 초기화 시드(seed) 값을 제공 받기 위해 실난수 발생기를 사용하지 않고는 안전성을 보장 받을 수 없다. 이러한 발생기는 그 시드(seed) 값이 완전한 랜덤성(randomness)을 제공하는 소스를 필요로 하나, 결정적인 시스템이라는 특성 때문에 완전한 랜덤성(randomness)을 제공하는 소스를 생성시키는 것이 현실적으로 불가능하다.

비결정적인 출력난수를 제공하는 실난수 발생기의 경우 동일하게 보편적인 하드웨어를 사용하는데, 그 특성상 속도가 느리고, 구현이 어렵기 때문에 난수 성능이 보장되지 않는 하드웨어라는 전제를 필요로 한다. 본 논문은 이러한 실난수 생성의 한계점들을 고찰하고, 키수열의 사후처리 과정에 요구되는 필터처리 방식에 대해 고찰하였다. 특히 고주파 필터나 라플라시안 필터 처리와 같은 방식을 출력열에 적용해 봄으로써 난수성에 어떤 영향을 받게 되는지를 살펴보았다.

관련 연구로는, Lacharme가 바이어스된 물리적인 난수 발생기를 위한 사후처리 함수에 대해 연구한 바 있고 [1], Barker 등은 결정적인 이진 난수 발생기를 사용한 난수 발생기법에 대한 표준에서 정의한 바 있다[2]. Dichtl은 사후처리된 물리적인 이진 난수의 나쁜 방법과 좋은

*교신저자 : Jin-Keun Hong
Tel: +82-10-3400-2445 e-mail: jkhong@bu.ac.kr
접수일 11년 12월 21일 수정일 (1차 12년 01월 19일, 2차 12년 02월 13일) 게재확정일 12년 03월 08일

방법이라는 주제로 연구함으로써, 물리적인 환경에서 생성되는 바이어스된 이진 난수에서 좋은 난수를 얻기 위한 방법에 초점을 맞추고 있다[3]. Pareschi 등[4]은 고체 물리회로에서 암호분야 적용을 위한 카오스 기반의 실난수 발생기에 대한 연구를 수행한 바 있고, Drutarovsky 등[5]은 재구성이 가능한 스위치 캐패시터 하드웨어에서 임베디드된 카오스 난수 발생기에 대해 연구하였다. Valtchanov 등[6]은 FPGA에 구현된 링 오실레이터에서 지터 모델링과 관측이라는 주제로 연구한 바 있고, Fischer 등[7]은 FPL에서 구현된 링 오실레이터의 보안성 개선이라는 측면에서 연구하였다. Varchola의 FPGA을 활용한 암호분야에서 최적화 설계와 평가나[8]를 포함한 주요 연구가 있었다, 본 논문에서는 상기 연구된 연구들에 대한 분석들을 기반으로, 하드웨어기반 이진 출력열의 난수 발생기에 영향을 미치는 주요 인자들을 분석하고, 이 가운데 암호 알고리즘, 부호 알고리즘 등을 적용하여, 난수성 정도가 어떤 영향을 받는지 살펴보았다.

본 논문은 2장에서 하드웨어 이진 난수 발생기 주요 요소와 난수성 평가 항목을, 3장에서 하드웨어 이진 난수의 출력 영향 인자에 대해 살펴보았으며, 4장에서 실험 및 결과, 마지막 5장에서 결론을 맺었다.

2. 하드웨어 이진 난수 발생기

2.1 하드웨어 이진 출력열 발생기 주요 요소

■ 가우시안 잡음원

가우시안 잡음 분포함수 $f(x)$ 의 확률밀도는 식(1)에서와 같이 정의할 수 있다.

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} \quad (1)$$

여기서 σ 는 가우시안 잡음전압의 실효 값이고 실난수 발생기의 잡음 전력밀도는 진폭이 가우시안 분포를 갖는다.

■ 엔트로피

랜덤 비트 발생기가 1/2 이상적인 값으로부터 확률을 이탈한 1비트를 생성한다고 할 때나, 생성된 발생 비트가 독립적이지 않다고 할 때, 다음에 발생한 비트는 추측하기 쉽다. 만일 확률이 주어진 환경의 이벤트가 유한한 집합이라면, 이때 엔트로피는 다음과 같이 정의할 수 있다.

$$-\sum_{i=1}^{n} p_i \cdot \ln(p_i) \quad (2)$$

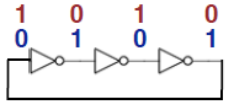
여기서 ln()는 2를 베이스로 하는 로그 값이다. m은 무한대 값이다. 비트의 종속성을 고려하여 이벤트로 m비트의 블록을 취급한다.

■ 플립플롭

기억소자의 출력이 현재의 입력에 의해서만 결정되지 않고, 과거의 입력상태의 값에 의해서 출력 값이 결정되는 논리구조의 시스템이 순차 또는 순서논리회로이다. 이 회로는 현재상태, 이전상태, 추후상태의 정보를 기반으로 정보를 저장할 수 있는 소자가 필요한데, 이때 가장 기본적인 기억소자를 플립플롭(flip-flop)이라 한다.

■ 발진기

일반적으로 하드웨어 잡음원 기반의 난수발생기에 적용되는 링 오실레이터는 MOSFET, Bipolar 등이 사용된다. 발진기에서 신호의 안정도는 신호가 시간이 지나면서 주파수 축 상에 고정되어야 하나, 실제 고정되지 않는 현상이 일어나게 된다. 증폭기의 경우 트랜지스터(TR)과 저항(R), 인덕터(L), 캐패시터(C)로 구성되지만, 발진기의 경우 공진기를 사용한다. 링 오실레이터는 회로 논리 구성에서 홀수로 구성된 인버터를 사용한다. 타이밍 정확도(지터)가 열잡음에 매우 민감하다. 0과 1 상태 사이를 발진하고, 전파 시간이 랜덤성에 기반하고 있다. 지터로부터 랜덤성 추출은 아날로그 오퍼레이션의 경우 다수 개의 XOR 발진기를 사용하고, 아날로그 신호 샘플링하며, 논리적으로 0이나 1을 적합한 시간(플랑크의 정확한 시간)이 가우시안인데 이 시간으로 강제로 추출하게 된다.



[그림 1] [0, 1] 발진 회로
[Fig. 1] Oscillator Circuits [0,1]

신호가 예기치 않는 곳에서 시간의 오차가 발생할 수 있다(fill rate). k 값과 l의 값을 튜닝하여 이를 조절할 수 있다. 그러므로 링 오실레이터는 인버터의 홀 수 개수로 구성되며, 다음 식과 같이 나타낼 수 있다.

$$f_{RO} = \frac{1}{2nd_{inv}} \quad (3)$$

여기서 f_{RO}는 RO의 주파수, n은 인버터의 개수, d_{inv}는 인버터의 지연 시간을 나타난다.

■ 메타 안정성 문제

오실레이터에서 메타 안정성 문제는 플립플롭의 홀드

조건이나 셋업 조건의 위반에 따라, 교차로 연결된 플립플롭의 내부 게이트 쌍이 논리적으로 high 또는 low 상태도 아닌 중간 상태로 전혀 예측되지 않은 방향으로 행동하거나 발진할 수 있다. 어떤 경우 발진이 사라지고, 난수성을 갖는 소스에 상승됨에 따라 플립플롭이 논리적으로 high 또는 low로 최종 안정화되기도 한다.

■ **탄성 함수 문제**

잡음원의 사후처리는 오류정정코드를 사용한 탄성함수를 이용하여 하기도 한다. m비트 랜덤비트 r[i]가 n비트 디지털화된 잡음 신호 s[i] (n>m)로부터 계산된다.

$$(r[i], ..., r[i+m-1])=(s[i], ..., s[i+n-1]) \cdot G^T \quad (4)$$

여기서 G는 [n, m, d] 선형 부호에 대한 생성 매트릭스이다. 순회 부호에 대해(선형 부호의 특정 클래스), 생성 다항식은 다음과 같이 표현할 수 있다. 탄성함수는 m비트 내에 m/n 압축 인자와 d-1 오류를 교정할 수 있다. 탄성함수는 잡음 소스에 의해 생성된 것 보다더 랜덤 비트를 교정할 수 있다. XOR 트리는 모든 링 오실레이터로부터 출력을 해시 처리하는 방안도 있다.

2.2 하드웨어 이진 난수 출력의 난수성 평가 항목

평가 방안들은 문턱치, 고정된 범위, 확률 값을 중심으로 평가하며, NIST의 경우, 단일 이진 시퀀스에 대해 단계별로 평가가 이루어지고 있다. 이 평가항목은 널 가정, 시퀀스 테스트 통계, P 값 계산, P 값 범위 비교에 대해 시행된다. 통계 테스트는 주기성, 누적 합, 런 검정(제일 긴 1의 수), 런, 랭크, 스펙트럴, 오버랩 되지 않은 템플릿 매칭, 오버레핑된 탬플릿 매칭, 유니버설 통계, 랜덤성 유지, 랜덤성 유지 변동폭, 근사 엔트로피, 시리얼, Lempe1-Ziv 복잡도, 선형복잡도 항목을 기반으로 난수성 평가 검증이 이루어지고 있는 실정이다. 본 논문에서는 주요 평가지수로, Frequency, serial, poker를 주요 평가지수로 사용하였다.

3. 하드웨어 이진 난수 출력영향 인자

하드웨어 이진 난수 발생기의 출력열에 영향을 미치는 주요 인자에는 지터, 온도와 같은 요소들이 있다.

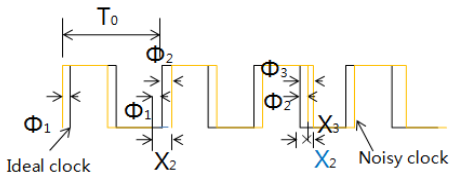
3.1 지터 요소

지터는 시간상에 이상적인 위치로부터 디지털 신호의 중요 인스턴스의 단기간 변이가 나타나는 것으로 정의한다. 지터는 결정적인 지터와 비결정적인 지터로 구분하며, 랜덤 지터는 가우시안 분포 즉 표준 변이가 시간에 따라 증가할 수 있는 분포를 기반으로 하는 것과 TRNG에 사용되는 비결정적인 지터가 있다. 지터는 주기 지터, 사이클대 사이클 지터, 하나의 사이클 지터와 시간 간격 오류 등으로 특징지어진다. 위상 지터는 주기 T_0을 갖는 이상적인 클럭으로부터 위상에 대해 클럭이나 오실레이터의 측정된 위상 사이의 차 값이다. 위상 측정은 nT_0 이산 시간 간격에 이루어진다. 위상 지터 Φ_n은 이상적인 주기 시간 $t=nT_o$와 측정된 시간 사이 차이다.

$$\Phi_n = t_n - nT_o \quad (5)$$

$$X_n = (t_n - t_{n-1}) - T_o = \Phi_n - \Phi_{n-1} \quad (6)$$

$$\Psi_n = (t_n - t_{n-1}) - (t_{n-1} - t_{n-2}) = X_n - X_{n-1} \quad (7)$$



[그림 2] 위상 지터Φ, 주기 지터X, 사이클대 사이클 지터 Ψ
[Fig. 2] Cycle jitter Ψ vs. phase jitter Φ and period jitter X

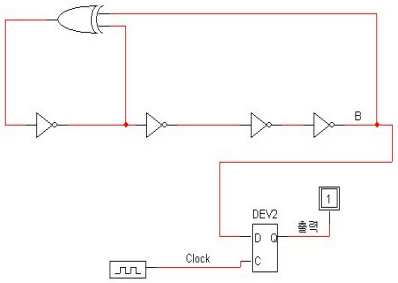
3.2 온도 요소

FPGA 온도에 안정화 요소에 대한 연구는 Fisher[9]이나 Schelleken[10] 등에 의해 수행된 바 있다. 이들 연구 결과에 따르면, FPGA온도 변이에 따라 TRNG 출력열의 난수성 평가 성공확률에 영향 정도를 분석하고 있다. 또한 FPGA 온도가 난수성 검증 항목 가운데, frequency 검증에서 비효율적인 반면, run 검증이나 poker 검증에서 TRNG 결함 여부와 연결되고 있음을 제시한다.

4. 실험 및 결과

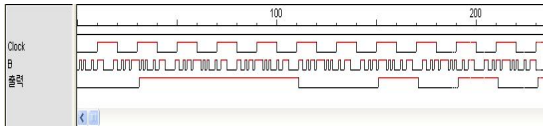
4.1 오실레이터 기반의 클럭, XOR 환경변이에 따른 출력 영향

그림 4는 디지털 하드웨어 발생기의 주요소로 구성되는 인버터 회로를 실험 예를 나타내었다.



[그림 4] 이진 난수 출력열을 생성하는 오실레이터 회로
[Fig. 4] Oscillator circuit generating binary random output stream

주어진 회로는 클럭과 XOR 게이트의 지연시간 변화에 따른 난수 출력 변이를 다음 그림 5와 표 1에서 제시하였다.



[그림 5] Clock(10,10), XOR게이트(1,1) 환경에서 출력파형
[Fig. 5] Output waveform in Clock(10,10) and XOR Gate(1,1) environment

[표 1] Clock(10,10), XOR게이트(1,1) 값의 출력
[Table 1] Output of Clock(10,10),XOR gate(1,1)

$T	$D	$O	"출력"	$O
36	2	1	0	1
38	1	1	1	1
39	1	1	0	1
40	1	1	0	0
41	3	1	1	0
44	5	1	0	0
49	1	1	1	0
50	1	1	1	1
51	2	1	0	1
53	1	1	1	1
54	1	1	0	1
55	2	1	1	1
57	1	1	0	1
58	2	1	1	1
60	2	1	1	0
62	1	1	0	0
63	1	1	1	0
64	1	1	0	0
65	1	1	1	0
66	3	1	0	0
69	1	1	1	0
70	2	1	0	1
72	3	1	1	1
75	5	1	0	1

표 2에서는 클럭 (10,10) 조건에서 XOR 게이트 시간을 가변시켜 나온 출력열을 비교한 것이다. XOR 게이트 시간을 어떻게 가변하는가에 따라 즉 지연시간의 가변 정도에 따라 난수성을 결정하는 출력열이 가변되고 있음을 확인할 수 있다. XOR 게이트 시간이 (20,20)인 경우가 "0', "1"의 패턴이 "1" 패턴이 연속으로 출력되는 (50,50), (85,85), (100,100)보다 frequency 특성 측면에서 좋음을 보이고 있다. 표 3에서는 클럭 지연 시간 변이에 따라 출력열이 "1"이 나올 확률(런 길이에 따라)을 분석한 것이다. 런 길이는 길이 수에 비례하여 일어날 확률이 $1/2^n$에 비례하는 특성을 갖는다. 실제 클럭 지연 요소는 런 길이 특성에도 영향을 미치고 있으며, 실제 오실레이터 설계시에 클럭 지연 요소가 함께 고려되어 최적의 지연 시간을 설정하는 것이 필요함을 알 수 있다.

[표 2] XOR Gate 지연시간 변이에 따른 출력
[Table 2] Output according to delayed time variation of XOR gate

1,1	2,2	3,3	4,4	5,5	10,10	15,15	20,20	30,30	50,50	85,85
0(2)	0(2)	1(2)	0(4)	0(4)	1(3)	0(2)	0(4)	0(2)	1(6)	1(2)
1	1	0	1(6)	1(6)	0(3)	1	1(6)	1	1(10)	1(!0)
0	0(2)	1	0	0	1(6)	0	1(9)	0(3)	1(7)	1(3)
0	1(4)	0(3)	0(2)	0(2)	0	0	0	1(6)	0(2)	0
1(3)	0	1	1(3)	1(3)	1	1	0(2)	1(9)	1	1(2)
0(5)	0	0	0(4)	0(4)	0(2)	0(3)	1(3)	0	0(2)	0(4)
1	1	1	0(5)	0(5)	0(4)	1	0(3)	1(2)	1	1
1	0(2)	0(2)	1(5)	1(5)	1(3)	0	1(2)	0(4)	0(2)	1(9)
0(2)	1(4)	1	1	1	0	1(3)	1(10)	1(4)	1	1(7)
1	0(2)	0(2)	0(3)	0(3)	1	0	0(10)	1	0(2)	0
0	1	1(5)	1(3)	1(3)	0	0(3)	0	0	1(2)	1(2)
1(2)	0(2)	0(2)	0(3)	0(3)	1	1(6)	0	1(2)	1(10)	0
0	1(4)	1	0(6)	0(6)	0	0(2)	1(8)	0(4)	1(10)	0(3)
1(2)	0(2)	1	1(4)	1(4)	1(3)	1	1	1(2)	1(10)	1(6)
1(2)	1	0(2)	1(2)	1(2)	0(4)	0	0(3)	1	1(8)	1(!0)
0	0	1	0(3)	0(3)	1	1	1(6)	1(9)	0(2)	1(10)
1	0	0	1(3)	1(3)	0(4)	0(4)	1	0	1(10)	1(10)
0	1(4)	1	0(2)	0(2)	1	1	1(2)	1(3)	0(2)	1(10)
1	0(2)	0	0(7)	0(7)	0(4)	0(3)	0(3)	0(2)	1(8)	1(9)
0(3)	1	1(2)	1(3)	1(3)	1	1(3)	1(4)	1	1(10)	0
1	0	0(3)				0(2)	1(2)	0(3)	1(10)	1
0(2)		1(2)				1(2)	0(6)		1(9)	1(2)
1(3)		0(4)					1(2)		0	0(2)
		1	1(3)	1(3)	0		1(4)			1
0(5)	0					0(2)	0(6)	1	0	0(3)
		0								1
							1(3)			1(10)

4.2 디지털입력에 알고리즘 결합에 따른 영향

표 4와 5에서 제시된 실험은 디지털 잡음 입력원과 기타 암호 알고리즘 A5, 부호화 알고리즘 ML(15,4), 그리고 기타 잡음을 추가한 정보에 난수성 검증을 실시한 결과이다. 실험결과 frequency 검증에서는 ML(15,4) 결합모델이 A5결합 모델보다 우수한 성능을 보이는 반면, serial이나 poker 검증에서는 A5 알고리즘이 우수하다.

5. 결 론

본 논문에서는 하드웨어 발생기의 디지털 입력원에 영향을 미치는 주요 인자에 대해 분석하였다. 오실레이터의 출력에 영향을 주는 지터에 대해 살펴보았으며, 지연된 클럭 지연 요소 영향정도를 살펴보았다. XOR 게이트 지연시간 변이에 따른 영향을 통해 설계시 지연시간 변이와 난수성을 고려하여 최적의 지연변이를 고려하여 설계의 필요성을 확인하였다. 또한 입력원을 잡음과 암호알고리즘 A5, 부호알고리즘 ML(15,4) 결합 모델로부터 난수성 영향을 분석하였다. 빈도검증에서는 ML결합모델이, 시리얼 검증에서는 A5결합모델이 우수한 성능을 보였다. 온도 영향이 난수성에 영향을 미치기 때문에 설계 시에 이 문제를 고려해야 함을 알 수 있었다. 향후 연구에서는 결합모델을 하드웨어 구현에서 최적화 방안을 연구하고자 한다.

[표 3] Clock 지연시간 변이에 따른 출력"1" 확률
[Table 3] Probability of output "1" according to variation of delayed clock time

"1"	1,1	2,2	3,3	4,4	5,5	10,10	15,15	20,20	30,30	50,50	85,85
1개	12/19	9/21	13/20	10/33	10/33	10/21	10/20	15/63	13/42	16/113	19/106
확률	0.43	0.51	0.46	0.45	0.45	0.44	0.43	0.43	0.61	0.67	0.89
연속2개	3		3	1	1		1	4	3	1	4
확률	0.13		0.14	0.03	0.03		0.04	0.08	0.09	0,02	0.06
연속3개	2			5	5	3	2	2	1		1
확률	0.14			0.21	0.21	0.2	0.13	0.06	0.05		0.03
연속4개		4		1	1			2	1		
확률		0.4		0.05	0.05			0.08	0.07		
연속5개			1	1	1						
확률			0.13	0.07	0.07						
연속6개				1	1	1	1	2	1	1	1
확률				0.08	0.08	0.14	0.14	0.12	0.1	0.05	0.05
연속7개										1	1
확률										0.06	0.06
연속8개								1		2	
확률								0.08		0.13	0.14
연속9개								1	2	1	2
확률								0.09	0.29	0.07	0.15
연속10개								1		6	6
확률								0.1		0.5	0.5
전체 1 개수	44	41	43	73	73	47	46	103	63	127	122

[표 4] 잡음과 알고리즘 결합정보의 난수성 검증
[Table 4] randomness evaluation according to combing noise data1 and algorithm

random test	입력	A5	ML (15,4)	입력+ 잡음	A5+ 잡음	ML(15,4) + 잡음
frequency	118346	201	7	935	110	2
serial	243744	369	333	1957	204	468
3-serial	485011	459	1033	2419	609	1272
4-serial	936777	521	2362	3026	976	2734
5-serial	1807076	12167	72482	74069	8164	72358
poker-3	282321	345	495	1770	307	667
poker-4	495863	3187	3796	18044	4215	3664
poker-5	718328	2766	15248	16489	2029	15300

[표 5] 잡음과 알고리즘 결합정보의 난수성 검증
[Table 5] Randomness evaluation according to combing noise data2 and algorithm

random test	원본+ 잡음2	A5+ 잡음2	ML(15,4) +잡음2	원본+ 잡음3	A5+ 잡음3	ML(15,4) +잡음3
frequency	494	62	5	900	117	10
serial	763	87	459	901	118	445
3-serial	2252	336	1356	1968	244	1293
4-serial	3434	510	2776	2212	285	2709
5-serial	29665	4751	71653	40176	6304	71616
poker-3	1171	163	71653	1260	160	643
poker-4	14977	2515	3674	14303	2280	3630
poker-5	7321	1137	14968	9245	1415	15374

References

[1] P. Lacharme, "Post-processing functions for a biased physical random number generator,"in Fast Software Encryption workshop - FSE 2008.

[2] E. Barker and J. Kelsey, "Nist special publication 800-90: Recommendation for random number generation using deterministic random bit generators,"National Institute of Standards and Technology (NIST), Computer Security Division Information Technology Laboratory, March 2007.

[3] M. Dichtl, "Bad and good ways of post-processing biased physical random numbers,"in Fast Software Encryption workshop - FSE 2007.

[4] F. Pareschi, G. Setti, and R. Rovatti, "A fast chaos-based true random number generator for cryptographic applications,"in Solid-State Circuits Conference, 2006.

ESSCIRC 2006. Proceedings of the 32nd European, September 2006, pp. 130-133.
[5] M. Drutarovsky and P. Galajda, "A robust chaos-based true random number generator embedded in recongurable switched-capacitor hardware," in Radio elektronika, 2007. 17th International Conference, April, pp. 1-6.
[6] B. Valtchanov, A. Aubert, F. Bernard, and V. Fischer, "Modeling and observing the jitter in ring oscillators implemented in fpgas,"in The 11-th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS), Bratislava, April 2008, pp. 158-163.
[7] V. Fischer, F. Bernard, N. Bochard, and M. Varchola, "Enhancing security of ring oscillator based rng implemented in fpga," in Field-Programable Logic and Applications (FPL), September 2008, pp. 245-250.
[8] M. Varchola, "Design and evaluation of optimized fpga ip-cores for cryptography," in Computer Architectures & Diagnostics (Pocitacove Architektury & Diagnostika - PAD), September 2008, pp. 113-118.
[9] *V. Fischer and M. Drutarovsk´y, "rue random number generator embedded in reconfigurable hardware," in CHES '2: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems. London, UK: Springer-Verlag, 2003, pp. 415–30.
[10] **D. Schellekens, B. Preneel, and I. Verbauwhede, "pga vendor agnostic true random number generator," in Field Programmable Logic and Applications, 2006. FPL '6, 2006, pp. 1–6.

홍 진 근(Jin-Keun Hong) **[정회원]**

- 2004년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전술통신, 센서넷, RFID, 무선랜 보안