실난수생성기에서 필터 윈도우크기에 관한 연구

Performance Analysis according to Filter Window Size in Random Number Generator Using Filter Algorithm

홍진근
천안대학교

Hong Jin-Keun
A Univ., Cheonan Univ.

요약

암호학에 적용되는 실난수 발생기는 기본적인 잡음 메카니즘으로부터 유도된 불예측적이고, 편이성을 가지지 않은 이진 수열을 요구한다. 본 논문에서는 하드웨어로 구현된 실난수 발생기가 편이성을 가진 출력수열을 통계적으로 제거하기 위해 필터기법을 사용한다. 사용된 필터처리기법에서 윈도우크기에 따른 손실율을 분석하여 적합한 윈도우 크기를 제안하고자 한다.

Abstract

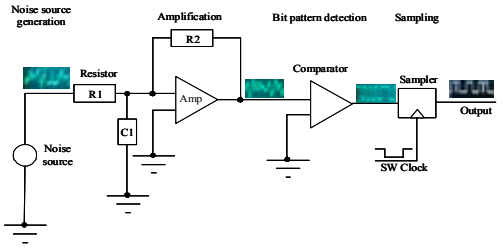
Critical cryptography applications require the production of an unpredictable and unbiased stream of binary data derived from a fundamental noise mechanism. In this paper, we proposed a RNG with Gaussian noise using filter algorithm. The proposed scheme is designed to reduce the statistical property of the biased bit stream in the output of a RNG. Experimental show that we analysis the loss rate according to window size and propose optimum window size.

I. 서 론

실난수 발생기는 데이터 암호나 통계적인 시뮬레이션, 추첨식 복권 등과 같은 분야에서의 사용이 증가하는 추세에 따라, 실난수 발생기와 의사난수발생기로 결합된 모델의 암호시스템이 구현되고 있다[1.] 실난수 발생기는 실난수 특성을 제공하기 위해 전자회로의 증폭 기법과 샘플링 기법을 사용하고, 이러한 방법은 자연계 현상으로부터 열잡음, 산탄잡음, 1/f잡음 등과 같은 신호들로부터 추출 것이 적합한 방법으로 알려져 있다[2]. 하드웨어로 구성된 실난수 발생기는 출력 수열이 편이셩을 가지지 않은 통계적 난수성을 제공하는 것이 매우 어려운 실정이다. 기존 연구는 H/W RNG와 해쉬함수(hash function)가 결합된 모델이나 PRNG가 결합된 모델을 이용함으로써 편이성을 가지고, 불안정한 실난수 발생기의 랜덤성 한계를 해결해 오고 있다[2-4]. 본 논문은 해쉬함수나 LFSR 결합 모델에 의존하지 않고, 실난수 발생기의 비주기적인 특성과 편이성을 가지지 않은 특성을 제공하기 위해 편이성을 가지는 출력수열을 제거하여 난수성을 높이는 필터 알고리즘을 적용하며, 이때 제안된 필터 윈도우 크기가 편이성을 지니는 손실율에 미치는 영향을 분석한다. 2장에서는 실난수 발생 발생메카니즘에 대해 설명한다. 3장에서는 필터처리에서 윈도우 크기의 영향에 대한 분석과 실험결과에 대해 살펴보고, 4장에서 결론을 맺는다.

II. 실난수 발생 메카니즘

실난수 발생기는 안정된 잡음원의 추출, 추출된 잡음원의 증폭, 증폭된 잡음원의 비교기를 통한 "1", "0" 패턴 식별, 및 샘플링 등의 과정으로 이루어진다. 잡음원 추출은 미약한 잡음 AC 신호를 검출하고, 이를 추출 가능한 크기로 사용하기 위해 증폭과정을 거친다. 이때 증폭은 연산증폭기를 사용한다.



▶▶ 그림 1. 실난수 발생기의 발생 메카니즘

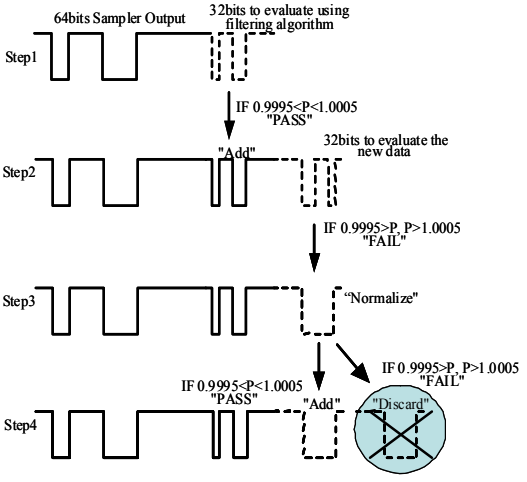
패턴식별과정에서는 제로교차점을 이용하는 비교기를 사용하여 AC 잡음신호를 "1", "0" 패턴으로 식별한다. 비교기 출력으로부터 얻어진 이진 비트열은 일정한 샘플링 주파수를 통해 샘플링 처리되어 난수열로 수집된다. 이때 수집된 난수열은 제안한 필터링 알고리즘을 이용해 non bias한 출력열로 필터링 된다. 시스템에서 적용된 잡음 다이오드는 Noisecom사의 NC201 모델이며 0.1Hz~10MHz 대역에서 백색 가우스 분포특성을 가진다. 비교기의 출력은 소프트웨어로 구현된 샘플러를 통해 처리되며, 상승에지에서 "0", "1" 패턴이 식별되어 얻어지고, 이때 적용된 비교기의 특성은 차동 아날로그 입력을 가지며, 능동적인 내부 풀업을 갖는 TTL 로직 출력을 제공한다. 또한 샘플링 회로는 빠른 전파 지연시간을 가지며, 편이성을 갖지 않도록 샘플링율이 조정되도록 설계되었다.

III. 필터처리에서 윈도우 크기의 영향

샘플링 처리되어 수집된 출력수열은 소프트웨어 필터처리를 통해 편이성이 제거된다. 필터 알고리즘은 출력 수열이 편이성을 가질 때 편이성을 제거하기 위해, 출력 수열을 임시 저장하기 위한 버퍼와 편이성 정도를 측정하는 기준인 유의수준에 따른 판별기준이 중요한 요소로 작용한다. 사용된 필터 알고리즘에서는 통과된 비트열을 저장하기 위해 사용되는 버퍼 크기는 16, 32, 64, 128, 256, 512를 수용 가능한 크기로 정해지며, 통과(PASS)/실패(FAIL)"를 결정하기 위해 사용되는 유의수준 레벨 결정 값은 0.9995~1.0005 범위로 정하였다.

$$P = \frac{S\{= \sum \#of collected\text{"}1\text{"}bits\}}{T\{= \#of collectedbitstream/2\}} \quad (1)$$

먼저, 샘플러 출력 비트열을 버퍼단위로 가져와 "1" 비트의 개수 합(S)을 구한다. 이 개수 합을 변수로 정의된 값에 저장하고, 수집된 길이의 절반 값(T)을 저장한다. 값은 "1" 개수 합인 값으로부터 구하고,



▶▶ 그림2. 필터 처리 흐름도

이때 얻어진 값이 검증 유의수준 범위 내에 있으면, 고정된 버퍼에 저장된 비트열은 통과된다. 값이 1에 근접하게 되면, 통과 확률이 높게 나타나게 되는데,

이는 "0"와 "1"의 비율 분포가 거의 비슷하게 나타나는 것을 의미한다. Step1에서 검증이 "통과(PASS)"하면 통과된 비트열은 비트열 저장을 위한 메모리에 추가되고, 만일 "실패(FAIL)"하면 검증을 위해 사용된 해당 비트열은 제거한다. 그림2에서 제시된 윈도우 크기는 64비트를 기준으로 하고 있다. 그러나 실난수 발생기의 특성과 성능에 따라 고정된 64비트를 활용하는 것은 비효율적이다. 출력 수열을 수집할 때 편이성을 가진 출력수열은 유의수준 결정기준에 근거하여 손실되고 이 손실되는 출력수열은 필터 윈도우 크기에 매우 민감한 요인으로 작용한다. 제시된 윈도우의 크기는 16비트, 32비트, 64비트, 128비트, 256비트, 512비트를 기준으로 하고 있다. 만일 윈도우의 크기 16비트 보다 512비트로 설정할 경우 손실되는 손실 확률은 512비트 윈도우 크기로 결정할 때보다 상대적으로 감소하나 1회 필터처리로 수집될 수 있는 양은 적다. 실난수 발생기 환경을 고려할 때 16비트 윈도우 크기보다 512비트의 원도우 크기로 결정하여 편이성을 측정할 때 512비트에서 유의수준 조건을 통과하는 수열을 얻기가 까다로우며, 1회 프로세싱에 얻을 수 있는 비트가 512비트 단위 기준이므로 주어진 시간에 얻을 수 있는 비트량이 16비트 단위로 얻을 수 있는 비트량에 비해 많을 수 있으나 손실 확률 또한 상대적으로 높고, 실난수의 난수성 기준에서 유의수준을 통과하기가 어렵다. 그러므로 실난수 발생기의 특성을 고려하여 윈도우 크기가 결정되어야 한다. 소요시간이 10초 동안 1million 필터 처리가 수행될 때,

[표 1] 필터 윈도우크기에 따른 전체 비트량

Filter window size	Generation bits	Loss bits	Passing probability (Win 16=99.9%)
Win= 16	1.6E+07	1.6E+04	99.9%
32	3.2E+07	6.4E+04	99.8%
64	6.4E+07	2.56E+04	99.6%
128	1.28E+08	1.02E+06	99.2%
254	2.56E+08	4.07E+06	98.4%
512	5.12E+08	1.61E+07	96.8%

표1에서 윈도우 크기 필터에 따라 얻어지는 전체 생성 비트량을 제시하였다. 윈도우 크기가 16으로 설정하여 해당 시간동안 얻을 수 있는 비트량은 1.6E+07 비트가 되고 이 가운데 성공할 수 있는 확률이 99.9%일 경우 1.6E+04 비트의 손실을 초래한다. 그런데 만일 윈도우의 크기를 증가시키면 생성되는 비트양이 증가하는 반면, 상대적으로 손실확률 또한 증가하게 되며, 동일한 출력 난수열에서 윈도우 크기가 증가할수록 성공확률이 상대적으로 낮아진다. 필터 윈도우 크기 16을 기준할 때, 99.9%의 성공확률은 갖는 출력난수열은 윈도우 크기 32로 설정할 때 99.8%, 64에서 99.6%, 128에서 99.2%, 512에서 96.8%의 값으로 상대적으로 성공확률이 떨어지며, 실험적으로 윈도우 크기 64비트로 설정할 때, 81.5% 성공확률을 가지는데 비해 512비트의 윈도우 크기로 설정하여 출력 수열에 대한 편이성 여부를 판정할 때 매우 낮은 성공확률을 가지므로 이 경우 손실확률은 매우 높게 나타난다. 이러한 난수발생기의 상태일 경우 윈도우 크기 512비트로 설정하는 것은 비효율적이다.

[표 2] 윈도우크기에 따른 성공확률

Win size	The passing probability/1min										
Win= 16	99.9	99.7	99.5	99	97	95	93	91	90	85	80
32	99.8	99.4	99	98	94	90	86	82	81	72.2	64
64	99.6	98.8	98	96	88.5	81.5	74.8	68.6	65.6	52.2	41
128	99.2	97.6	96.1	92.3	78.4	66.3	56	47	43	27.2	16.8
254	98.4	95.3	92.3	85.1	61.4	44	31.3	22.1	18.5	7.4	2.8
512	96.8	90.8	85	72.5	37.7	19.4	9.8	4.9	3.4	0.5	0

윈도우 크기에 따른 성공확률, 소요시간 사이의 관계를 검토하면, 윈도우 크기 16으로 설정할 때 1회 프로세싱을 통해 얻을 수 있는 비트량은 16비트, 이에 반해 512비트를 윈도우 사이즈로 결정할 때 1회 프로세싱을 통해 얻을 수 있는 비트량은 512비트 단위이다. 그러므로 손실율을 고려하지 않는 다면 일반적으로 윈도우 크기를 증가시킴으로써 짧은 시간에 많은

양의 출력수열을 얻을 수 있다.

표3에서는 윈도우 크기에 따른 성공확률을 기준으로 할 때 성공확률을 비교하였다. 성공확률이 99% 환경에서 윈도우 크기를 512로 정하면 1분이 소요되는 반면 16으로 결정하면 23.5분의 시간이 소요된다. 그런데 윈도우 크기가 256비트로 설정할 경우 1.7분이 소요되고, 상대적으로 성공확률이 95% 수준으로 떨어질 경우 윈도우 크기가 256에서 0.9분인데 반면에 윈도우 크기 512의 경우 1분이 소요된다. 이것은 윈도우 크기를 증가시킬 경우 성공확률이 감소하는 환경에서는 오히려 손실량이 증가하므로 윈도우 크기가 512비트보다 256비트로 설정하는 것이 효율적인 것을 의미한다. 그러므로 소요시간, 성공확률에 따른 손실량, 단위시간에 얻을 수 있는 출력수열 수집량을 고려할 때 설계된 실난수 발생기의 경우 윈도우 크기를 출력 난수열의 특성에 따라 64비트, 128비트의 수준에서 결정되는 것이 효율적이다.

[표 3] 윈도우크기에 대한 성공확률과 소요시간 비교

Filter window size	Win=16, pass prob=99%	Win=16, pass prob=95%
Win=16	23.5min	6.5min
32	11.8min	3.4min
64	6min	1.9min
128	3.1min	1.2min
256	1.7min	0.9min
512	1min	1min

IV. 결 론

암호학에 적용되는 실난수 발생기는 기본적인 잡음 메카니즘으로부터 유도된 불예측적이고, 편이성을 가지지 않은 이진 수열을 요구한다. 본 논문에서는 하드웨어로 구현된 실난수 발생기가 편이성을 가진 출력수열을 통계적으로 제거하기 위해 필터기법을 사용한다. 사용된 필터처리기법에서 윈도우크기에 윈도우 크기, 성공확률에 따른 손실율, 소요시간을 분석하였다. 실험적으로 설계된 실난수 발생기의 경우 발생기의 상태에 따라 필터 윈도우 크기를 64비트, 128비트 수준에서 결정하는 것이 효율적이다.

▌참고문헌▐

[1] C. S. Petrie and J. A. Connelly, "A Noise-Based Random Bit Generator IC for Applications in Cryptography," Proc. ISCAS'98, June 1998.

[2] http://www.io.com/~ritter/RES/NOISE.HTM.

[3] http://www.clark.net/pub/cme/P1363/ranno.html.

[4] http://webnz.com/robert/true_rng.html.

[5] W. Timothy Holman, J.Alvin Connelly, and Ahmad B. Dowlatabadi, "An Integrated Analog/Digital Random Noise Source," IEEE Transactions on Circuits and System I: Fundamental Theory and Applications, vol.44, no.6, June 1997.

[6] FIPS 140-1, "Security Requirements for Cryptographic Modules,"[Federal Information Processing Standards Publication 140-1], U.S. Department of Commerce /NIST[National Technical Information Service] Springfield, Virginia,1994. http://csrc.ncsl.nist.gov/fips/fips1401.htm (16 Oct. 1998).

[7] "Diehard," http://stat.fsu.edu/~geo/diehard.html (16 Oct. 1998).

[8] M. Delgado-Restituto, F. Medeiro, and A. Rodriguez- Vasquez, "Nonlinear switched-current CMOS IC for random signal generation," IEE electronic letters, vol. 29, December 1993.

[9] Habutsu, Y. Nishio, I. Sasase, S. Mori, "A Secret Key Cryptosystem Using a Chaotic Map," Trans. IEICE, vol. E73, no.7 July 1990.

[10] W. Timothy Holman, J. Alvin Connelly, Ahmad B. Dow latabadi, "An Integrated Analog/Digital Random Noise Source, "IEEE Trans. On circuits and systems -1:fundamental theory and applications, vol. 44, no. 6, June 1997.

[11] P. Elias, "The efficient construction of an unbiased random sequence," Ann. Math. Statist., vol. 43, no. 3, 1972.

[12] Boris Ya, Ryabko and Elena Matchikina, "Fast and Efficient Construction of an Unbiased Random Sequence," IEEE Trans. on information theory, vol. 46, no. 3, May 2000.