이미지센서 기반 진난수생성기에 적용 가능한 효율적인 엔트로피 축적 방법

유현도[2], 최영락[2], 강주성[1,2], 염용진[1,2]*
국민대학교 정보보안암호수학과[1] / 금융정보보안학과[2]
{dbguseh111, alpha1996, jskang, *salt}@kookmin.ac.kr

An applicability analysis of efficient entropy accumulation procedures to image sensor-based true random number generators

Hyeondo Yoo[2], Youngrak Choi, Ju-Sung Kang[1,2], Yongjin Yeom[1,2]*

Dept. of Information Security, Cryptology, and Mathematics[1]
Financial information security[2], Kookmin Univ.

요 약

암호학적으로 안전한 난수발생기로부터 출력된 수열의 난수성은 난수열 생성의 근원이라 할 수 있는 물리적 잡음원에 기인한다. 물리적 잡음원으로부터 생성된 원천적인 난수열은 일반적으로 엔트로피가 낮기 때문에 진난수생성기 내에서 엔트로피 축적 과정을 거치게 된다. 본 논문에서는 해쉬함수 등의 암호학적 알고리즘을 사용하는 일반적인 축적 방법이 아닌 단순 순열 연산 기반의 매우 효율적인 엔트로피 축적 과정에 대하여 논한다. Windows 10에 내장된 엔트로피 축적 과정에 관한 난수성을 분석한 Dodis 등(Crypto2021)의 연구결과를 물리적 잡음원으로 이미지센서를 사용하는 진난수생성기에 적용하기 위한 세부 메커니즘을 제안한다. 더욱이 시뮬레이션 결과를 바탕으로 NIST의 최소 엔트로피 기준을 만족하기 위해 필요한 순열 연산의 반복 횟수와 엔트로피 축적 속도를 제시한다.

Ⅰ. 서 론

암호학적으로 안전한 난수발생기(Cryptographically Secure Random Number Generator)의 핵심 구성요소인 진난수생성기(True random number generator, TRNG)는 물리적 잡음원(Noise source)으로부터 엔트로피를 추출하여 난수를 생성한다.[1] 일반적인 진난수생성기는 해쉬함수를 이용하여 엔트로피를 축적한다. Dodis는 지난 Crypto 2021에서 해쉬함수를 사용하지 않는 순열(permutation) 연산 기반의 효율적인 엔트로피 축적 과정과 얻을 수 있는 최소 엔트로피의 하한을 제시하였다.[2]

본 논문에서는 이미지센서 기반 진난수생성기에 Dodis가 제안한 순열 연산 기반의 엔트로피 축적 과정을 적용하기 위한 세부 메커니즘을 제안한다. 또한 제안한 메커니즘을 통해 시뮬레이션한 결과를 바탕으로 NIST의 최소 엔트로피 기준을 만족하기 위해 필요한 순열 연산의 반복 횟수와 엔트로피 축적 속도를 제시한다.

Ⅱ. 선행 연구

지난 Crypto 2021에서 Dodis는 순열 연산 기반의 엔트로피 축적 과정을 통해 출력된 난수열의 최소 엔트로피 하한을 수학적으로 증명하였다.[2] 증명과정에서 2-monotone 분포와 Covering number라는 개념을 정의한다. 2-monotone 분포란 정의역이 단조구간 2개로 나누어지는 확률분포를 의미하고 Covering number는 엔트로피 축적 과정에서 사용하는 순열의 효율성을 측정하기 위해 정의한 개념이다.

정의. 순열 $\pi : \{0,1,..n\} \rightarrow \{0,1,..n\}$, $1 \le k \le n$에 대하여 Covering number $C_{\pi,k}$는 다음을 만족하는 가장 작은 자연수 m이다.

- $\{\pi^{\ell}(j) : 0 \le j < k, 0 \le \ell < m\} = \{0,1,..n\}$

n-bit 순열 π를 엔트로피 축적에 사용할 때 Dodis가 수학적으로 증명한 최소 엔트로피 $H_{\min}(D_{\pi}^{(\ell)})$의 하한은 다음과 같다.[2]

- D : 엔트로피 축적 과정에 사용되는 최소 엔트로피 $k = H_{\min}(D)$가 2 이상인 2-monotone 분포의 클래스 (D의 원소들은 서로 독립)
- m : 순열 π의 Covering number $C_{\pi,k}$
- ℓ : π 연산 반복 횟수 ($\ell \ge m$)
- $D_{\pi}^{(\ell)}$: D의 원소들과 π 연산을 ℓ번 사용하여 얻은 난수열의 분포

$$H_{\min}(D_{\pi}^{(\ell)}) \ge n(1-2^{\frac{k}{2}-\frac{k\ell}{2m}}). \quad (1)$$

또한, 비트 반전(bit reversed)을 의미하는 순열 tor을 사용할 경우 최소 엔트로피 $H_{\min}(D_{tor}^{(\ell)})$의 하한은 다음과 같다.[2]

$$H_{\min}(D_{tor}^{(\ell)}) \ge n(1-2^{-\frac{k^2\ell}{4n}}). \quad (2)$$

본 논문에서는 NISP SP 800-90B에서 제공하는 True random 8bit 데이터의 최소 엔트로피 측정 결과인 7.86을 Full Entropy로 정의하고 엔트로피 검정 기준으로 사용한다.[1] 또한, 위 두 식을 통해 이미지센서 기반 난수발생기가 rot 순열과 tor 순열을 사용하여 엔트로피 축적을 할 경우 Full Entropy를 축적하기 위해 반복해야 하는 연산 횟수를 각각 제안한다. rot는 Rotate then left를 의미하는 순열로 n-bit 입력을 α-bit ($1 \le \alpha < n$)만큼 왼쪽으로 이동 시킨 값을 출력한다. tor는 $i(\in[0,1,..n-1])$의 이진수 표현의 비트 반전을 입력으로 받아 $i+1 (\mathrm{mod} n)$의 이진수 표현의 비트 반전을 출력하는 순열이다.[2]

Ⅲ. 이미지센서 기반 진난수생성기 분석

이미지센서 기반 진난수생성기는 이미지센서의 OBP(Optical Black Pixel)를 물리적 잡음원으로 사용한다.[3] 실험의 사용한 이미지 센서 'PV 4209K'의 전체 OBP의 개수는 6*1920개 이며, 각 OBP는 한 번에 2비트 데이터를 전송한다. 따라서 전체 OBP가 전송하는 데이터는 n = 23,040-bit 크기의 비트열로 볼 수 있다. 본 논문에서는 Dodis의 연구결과를 이미지센서 기반 진난수생성기에 적용하기 위한 메커니즘으로 다음 확률변수 X_i, Y_j를 정의한다.

표본공간이 $\Omega := \{$전체 OBP에 의해 생성된 비트열 $\vec{x} = x_1x_2...x_n\}$ 일 때 ($\{x_{2i-1}x_{2i}\}$는 i번째 픽셀이 전송하는 2비트를 의미함), i 번째 OBP가 전송하는 2-bit를 정수로 표현한 확률변수를 $X_i := 2x_{2i-1} + x_{2i}$라 정의한다 ($1 \le i \le \frac{n}{2}$). OBP가 전송하는 2-bit 4개를 연접하여 만든 8-bit 데이터를 정수로 표현한 확률변수를 $Y_j := 2^6X_{4j-3} + 2^4X_{4j-2} + 2^2X_{4j-1} + X_{4j}$라 정의 한다.($1 \le j \le \frac{n}{8}$)

Claim 1: Y_j분포의 클래스는 다음 조건을 만족한다.

조건 ① : 각 Y_j가 서로 독립이어야 한다.

: 각 OBP는 독립적으로 생성된 비트를 전송하므로 X_i는 서로 독립이라 할 수 있고 이에 따라 Y_j 역시 서로 독립이라 할 수 있다.

조건 ② : 각 Y_j의 최소 엔트로피 k가 2이상의 값을 가져야 한다.

: 최소 엔트로피 측정 도구인 NIST SP 800-90B를 통해 Y_j의 최소 엔트로피가 약 3.36의 값을 갖는 것을 확인했다.[1]

조건 ③ : Y_j의 확률분포는 2-monotone 이다.

: Y_j의 확률분포는 이산분포이기 때문에 2-monotone 분포를 따른다고 가정할 수 있다.

Claim 1에 따라 이미지센서 기반 진난수생성기에 Dodis의 연구결과를 적용할 수 있다.

Ⅳ. 엔트로피 축적 과정 적용

Y_j의 최소 엔트로피가 약 3.36이므로 4장에서는 Y_j의 최소 엔트로피 k가 3 이상의 값을 가짐을 전제로 분석을 진행한다. 순열 연산 기반의 엔트로피 축적 과정은 사용하는 순열에 따라 Full Entropy 축적까지 필요한 연산 반복 횟수가 다르다. 본 논문에선 8-bit 데이터를 3-bit 씩 왼쪽으로 이동시키는 rot 순열과 8-bit tor 순열을 사용한다. 순열 연산을 사용하여 엔트로피를 축적할 때 마다 새로운 엔트로피 입력으로 OBP가 전송한 23,040-bit 크기의 비트열에서 순차적으로 8-bit를 사용한다.

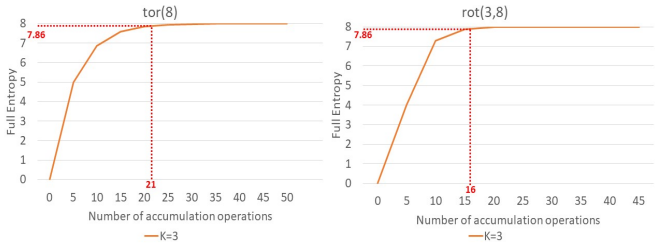
Algorithm 1. 이미지센서 기반 진난수발생기의 엔트로피 축적 과정

Input	$IV \in \{0,1\}^8$, 정수 ℓ ($\ge m$), OBP가 전송한 23,040-bit 크기의 비트열 $\vec{x} = x_1x_2...x_n$
Output	$IV \in \{0,1\}^8$
1	for $i \leftarrow$ 1 to ℓ do
2	$IV \leftarrow$ Permutation(IV)
3	$IV \leftarrow IV \oplus x_{8i-7}x_{8i-6}...x_{8i}$
4	end for
5	return IV

Ⅴ. 엔트로피 축적 과정 적용 결과 및 속도 측정

[그림 1]은 순열별로 엔트로피 축적 연산 반복 횟수에 따라 보장되는 최소 엔트로피를 나타낸다. 왼쪽 그래프는 8-bit tor 순열을 사용했을 때 Full Entropy 축적까지 필요한 연산 반복 횟수를 식 (2)를 통해 계산한 결과이다. 이는 식 (2)를 통해 계산한 결과이다. 오른쪽 그래프는 rot 순열을 사용했을 때 Full Entropy 축적까지 필요한 연산 반복 횟수를 식 (1)을 통해 계산한 결과이다.

[그림 1]에 표시되어 있듯 rot 순열을 엔트로피 축적 과정에 사용할 때, 연산을 16번 반복하면 Full Entropy에 도달할 수 있고, tor 순열을 엔트로피 축적 과정에서 사용할 때는 연산을 21번 반복할 때 Full Entropy를 얻을 수 있다.



[그림 1] 연산 반복 횟수에 따라 보장되는 최소 엔트로피

마지막으로 제안한 순열별 연산 반복 횟수를 통해 Full Entropy를 축적하는 속도를 계산한다. 이미지센서 기반 난수발생기의 FPS(Frame Per Second)는 6으로 설정되어 있기 때문에 1초에 17,280개의 8-bit 데이터를 사용할 수 있다.[3]

rot 순열을 사용하여 엔트로피를 축적할 경우 16개의 새로운 8-bit 엔트로피 입력이 필요하고 따라서, 약 8.5kbps의 엔트로피 축적 속도를 갖는다. tor 순열을 사용하여 엔트로피를 축적할 경우 21개의 새로운 8-bit 엔트로피 입력이 필요하고 따라서, 약 6.5kbps의 엔트로피 축적 속도를 갖는다.

Ⅵ. 결론

본 논문에서는 Dodis가 Crypto 2021에서 제안한 효율적인 엔트로피 축적에 관한 연구를 이미지센서 기반 난수발생기에 적용했다. rot 순열을 사용해 Full Entropy를 축적하기 위해서는 16번 연산을 반복해야 하고 tor 순열을 사용할 때는 21번 연산을 반복해야 함을 제시하였다. 마지막으로 Full Entropy 축적 속도의 경우 rot 순열은 약 8.5kbps, tor 순열은 약 6.5 kbps 정도일 것으로 추정하였다.

ACKNOWLEDGMENT

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로
한국연구재단-기후변화대응기술개발 사업(1711153545)과
과학기술일자리진흥원-과학치안 공공연구성과 실용화 촉진 시범사업의
지원을 받아 수행된 연구임(1711174177)

참 고 문 헌

[1] M. S. Turan, et al. "Recommendation for the Entropy Sources Usedfor Random Bit Generation", (Second DRAFT) NIST Special Publication 800 - 90B, 2016.

[2] Y. Dodis, et al. "No Time to Hash: On Super-Efficient Entropy Accumulation". In: Annual International Cryptology Conference. Springer, Cham, 2021. p. 548-576.

[3] Byung Kwon Park, Hojoong Park, Yong-Su Kim, Ju-Sung Kang, Yongjin Yeom, ChangHui Ye, Sung Moon, and Sang-Wook Han, "Practical True Random Number Generator using CMOS Image Sensor Dark Noise", IEEE Access, vol. 7, 2019.