Laboratorium Bezpieczeństwa Systemów Teleinformatycznych (cz.1)

Wykonał: Rafał Olszyna, nr albumu 139991

Data oddania: 12.04.2021

Podstawa opracowania

1. M. Hamburg, P. Kocher, M. E. Marson "ANALYSIS OF INTEL'S IVY BRIDGE DIGITAL RANDOM NUMBER GENERATOR" 2012
2. J. P. Mechalas "Intel® Digital Random Number Generator (DRNG) Software Implementation Guide" 2018

Systematyczny przegląd literatury:

1. E-zasoby Politechniki Poznańskiej
2. Słowa kluczowe: True Random Number Generator, ivy bridge
3. Wynik: P. Czernik, W. Winiecki, „Pomiary losowości danych wytwarzanych przez generator wbudowany w procesory firmy Intel z rodziny Ivy Bridge"
4. Wyszukanie w wyszukiwarce internetowej google: Intel RDRAND
5. Przejście na stronę en.wikipedia.org/wiki/RDRAND
6. Przejście na strone web.archive.org
7. Przejście na stronę software.intel.com
8. Zdefiniowany kod algorytmu

Analiza źródła entropii:

Intel RDRAND wykorzystuje sprzętowy generator źródła entropii.

Źródło Entropii (ES) działa asynchronicznie na samoczynnie regulowanym obwodzie i wykorzystuje szum termiczny w krzemie do generowania losowego strumienia bitów z częstotliwością 3 GHz.

Metoda poprawy właściwości statystycznych:

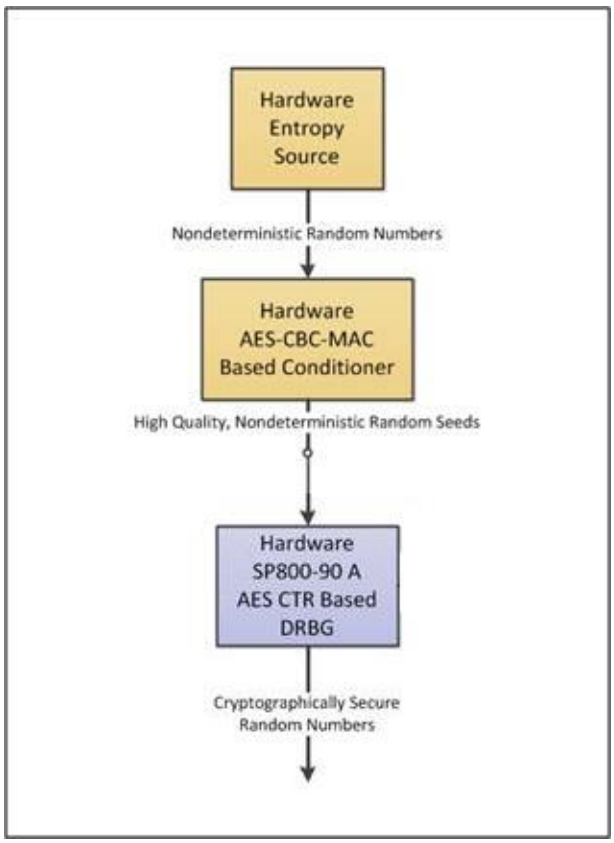
Bity o wartościach z przedziału 0-1 ze źródła entropii (ES) są przekazywane do kondycjonera w celu dalszego przetwarzania.

Kondycjoner pobiera pary 256-bitowych próbek entropii wygenerowanych przez źródło entropii i redukuje je do pojedynczej 256-bitowej próbki entropii przy użyciu algorytmu AES-CBC-MAC. Powoduje to zagęszczenie entropii do bardziej skoncentrowanych próbek

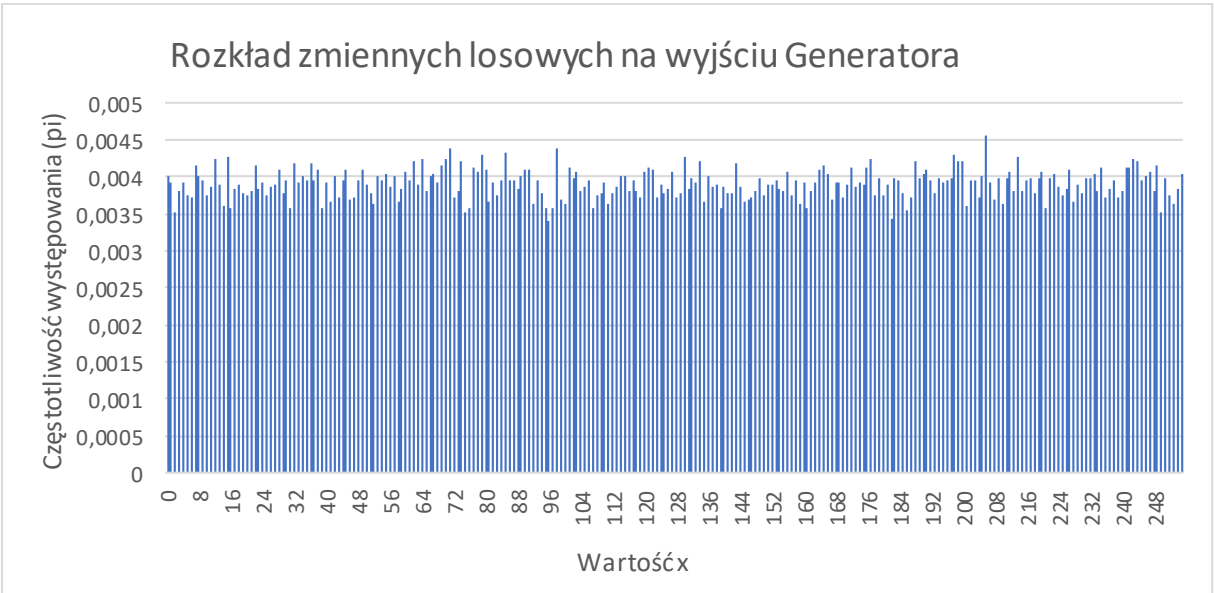
Entropia jest wyprowadzana jako wartość 256-bitowa i przekazywana do następnego etapu, gdzie jest wykorzystywana jako wartość losowa dla deterministycznego generatora bitów losowych (DRBG).

Rolą deterministycznego generatora bitów losowych (DRBG) jest "rozprowadzenie" warunkowej próbki entropii do dużego zbioru wartości losowych, zwiększając w ten sposób ilość liczb losowych dostępnych przez moduł sprzętowy. Odbywa się to poprzez zastosowanie DRBG zgodnego ze standardami i ciągłe zasilanie go uwarunkowanymi próbkami entropii.

Generator ten autonomicznie decyduje kiedy musi być ponownie załadowany nową liczbą losową aby odświeżyć własną pulę liczb losowych w buforze. Jednorazowo z jednej próbki wartości losowej może być wygenerowane maksymalnie 1022 liczb losowych na wyjściu generatora.



Schemat działania instrukcji Intel RDRAND



Entropia wyliczona zgodnie ze wzorem: $e = -\sum i\ p_i\ log_2(p_i)$ wynosi **7,947862 bita**

Uwagi:

- Brak możliwości wyliczenia entropii przy analizie źródła entropii z racji gotowej implementacji Intela!
- Pomiar wykonywany był na sprzęcie:
  Procesor: Intel Xeon E3-1245 v2,
  Ram: 2x4GB 1333Mhz
  Dysk SSD Crucial MX-500, 1TB, SATA
  temperatura otoczenia testów 22 stopnie, procesor 30 stopnie Celsjusza
- Środowisko programowania Code::Blocks 20.03, kompilator MinGW, do obliczeń wykorzystano środowisko Mircrosoft Excel
- **Program został zmodyfikowany o dodatkowe obcięcie próbek z przedziału wartości 0 - 4 294 967 295, za pomocą dzielenia modulo 256 każdej z otrzymanej próbki.**
- Prędkość działania generatora wraz z modyfikacją modulo
  100 000 wygenerowanych liczb – 0.490s
  1 000 000 liczb – 4.185s
  10 000 000 liczb – 42.688s
  100 000 000 liczb – 441.760s
- **Temperatura procesora nie wpływa w żaden sposób na losowość generowanych liczb**
  - 4 testy po 100 000 liczb, temperatura otoczenia 23 stopnie, syntetyczne obciążenie procesora programem linpack (w celu uzyskania wysokiej temperatury procesora), temperatura procesora **74 stopnie,** obliczenia widoczne w arkuszu „stress" dołączonego pliku .xlsx
    Uzyskane entropie:
    - 7,905736901
    - 8,051219761
    - 7,965784285
    - 8,070481663
  - 4 testy po 100 000 liczb, temperatura otoczenia 16 stopnie, syntetyczne obciążenie procesora programem linpack (w celu uzyskania wysokiej temperatury procesora), temperatura procesora **23 stopnie**, obliczenia widoczne w arkuszu „odpoczynek"
    Uzyskane entropie:
    - 7,888541286
    - 7,983931631
    - 8,066608654
    - 8,051219761