Generowanie ciągów bitów losowych z wykorzystaniem sygnałów pochodzących z komputera

Praca dyplomowa magisterska

Opiekun: prof. nzw. Zbigniew Kotulski

Andrzej Piasecki

apiaseck@mion.elka.pw.edu.pl

Plan prezentacji

1. Motywacja
2. Wprowadzenie
3. Architektura generatora
4. Analiza dysku twardego jako źródła entropii
5. Pytania

Motywacja

- Losowość jest niezbędnym elementem kryptografii
  - Proces generowania kluczy
- Twórcy algorytmów, protokołów kryptograficznych często zakładają dostępność nieskończonego strumienia bitów losowych
  - Każda sesja TLS wymaga 384 bitów losowych
  - Wygenerowanie klucza 1024 bitowego do RSA wymaga statystycznie ok. 100 – 200 Kb.

Entropia

- Entropia jest to średnia ilość informacji przypadająca na znak symbolizujący zajście zdarzenia z pewnego zbioru. Zdarzenia w tym zbiorze mają przypisane prawdopodobieństwa wystąpienia.

$$H(x) = \sum_{i=1}^{n} p(i) \log_r \frac{1}{p(i)}$$

- W teorii informacji najczęściej stosuje się logarytm o podstawie r=2, wówczas jednostką entropii jest bit.
- Entropię można interpretować jako niepewność wystąpienia danego zdarzenia elementarnego w następnej chwili.

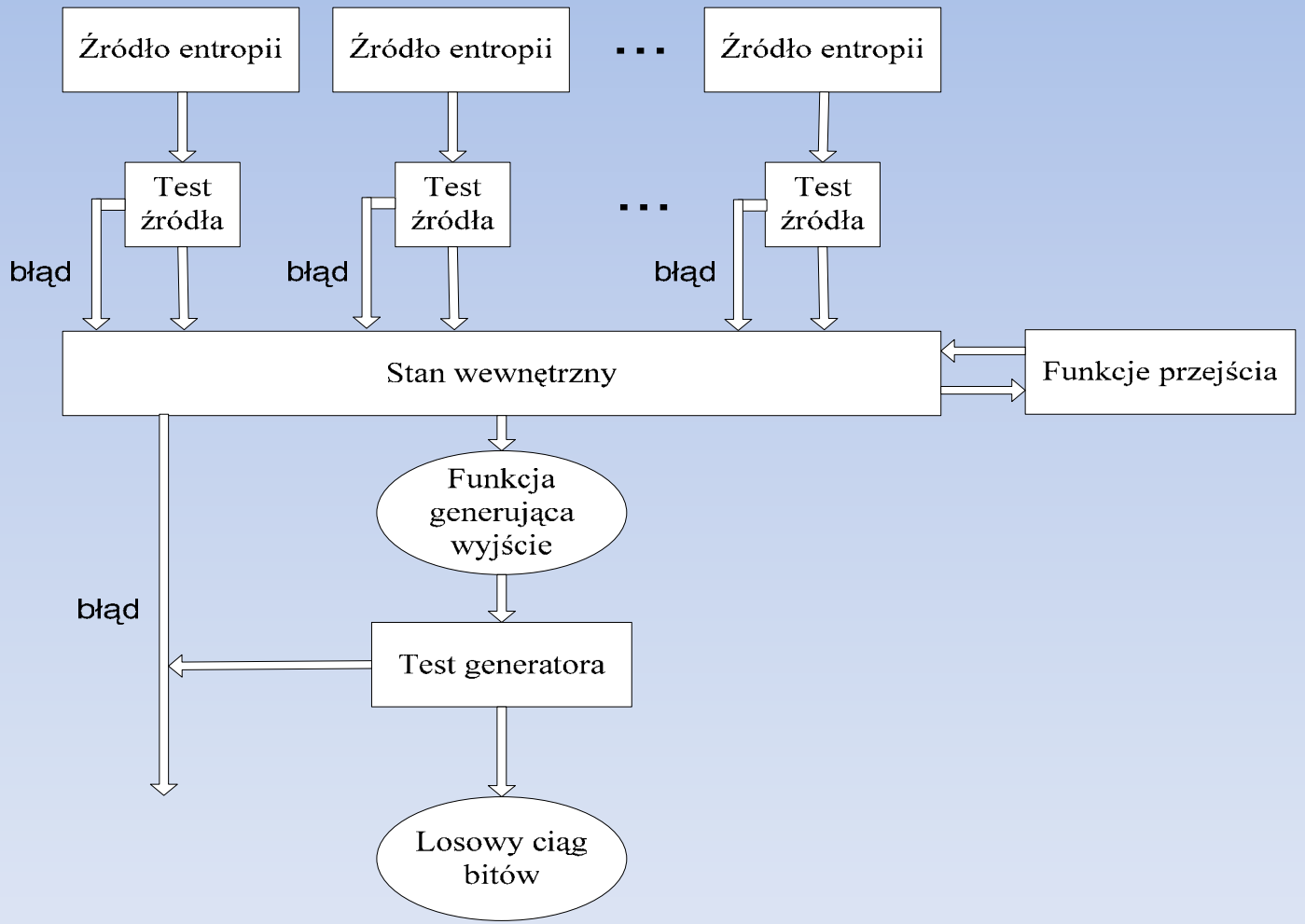
Wymagania stawiane generatorom bitów losowych

- nieprzewidywalny – nie wiadomo czy następnym bitem będzie 1 v 0
- bezstronny – 0 i 1 są jednakowo prawdopodobne
- niezależny – bity są nieskorelowane

Podział generatorów bitów losowych

- Deterministyczne - DRBG
  - Wykorzystują deterministyczne algorytmy do wygenerowania *pseudolosowej* sekwencji bitów z wejściowej, losowej sekwencji bitów nazywanej *ziarnem*
- Niedeterministyczne - NRBG
  - Wykorzystują źródła entropii, z których pobierana jest odpowiednia ilość entropii, potrzebna do wygenerowania z niej, algorytmami deterministycznymi, losowej sekwencji bitów.

Schemat NRBG



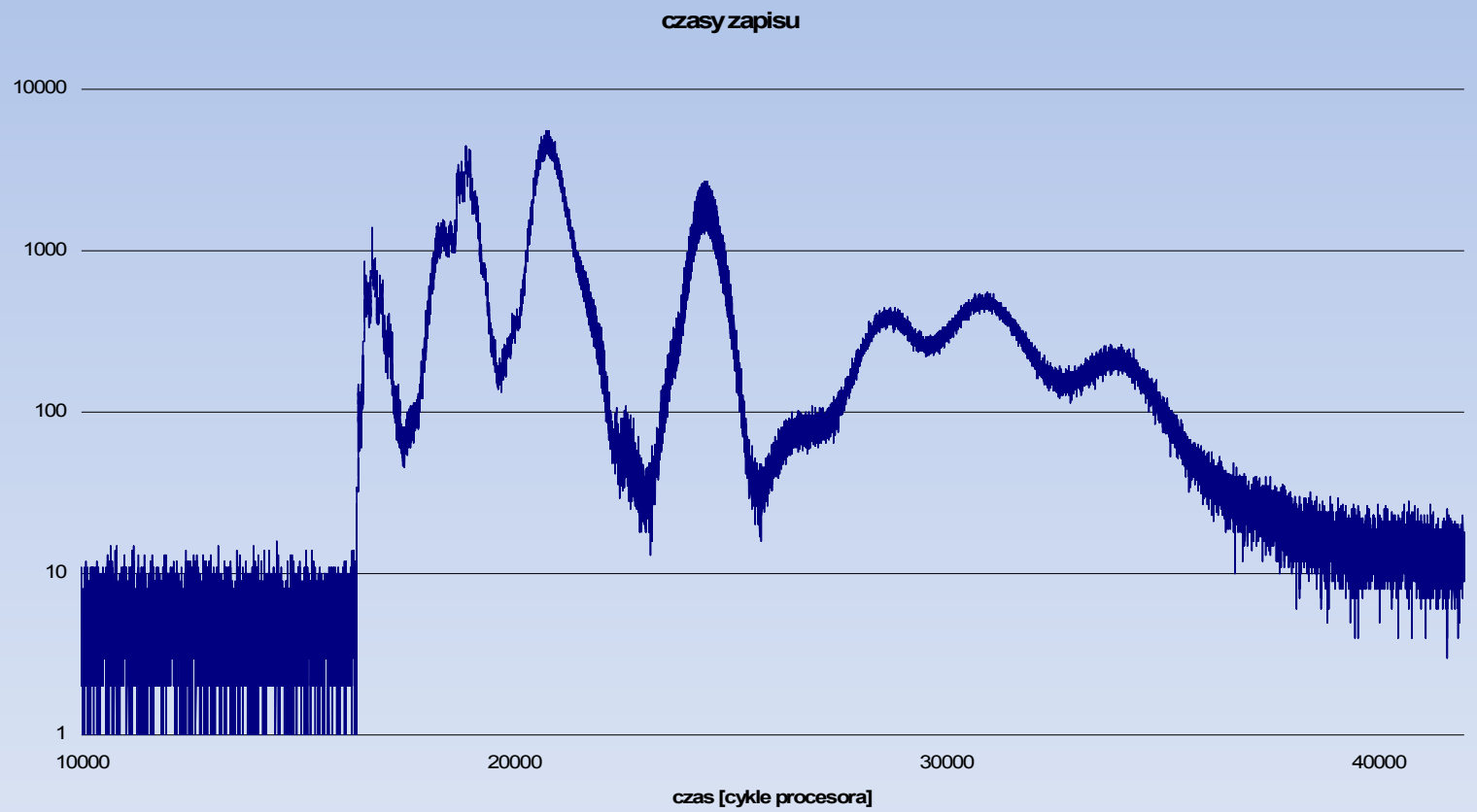
Źródła entropii

- *Sprzętowe*
  - Czas między emisjami cząsteczek w czasie rozpadu radioaktywnego
  - Szum termiczny diody półprzewodnikowej lub rezystora
  - Niestabilność częstotliwości własnej oscylatora
  - **Turbulencje powietrza w zamkniętym napędzie dyskowym, powodujące losowe fluktuacje czasów oczekiwania na odczyt/zapis danych**
  - Dźwięk z mikrofonu lub sygnał wizyjny z kamery
  - Czas między uderzeniami w klawisze (użytkownik)
  - Ruch myszy (użytkownik)
- *Programowe*
  - Zegar systemowy
  - Treść aktualnie wyświetlanego obrazu.
  - Statystyki systemu operacyjnego
  - Zawartość pamięci podręcznej procesora

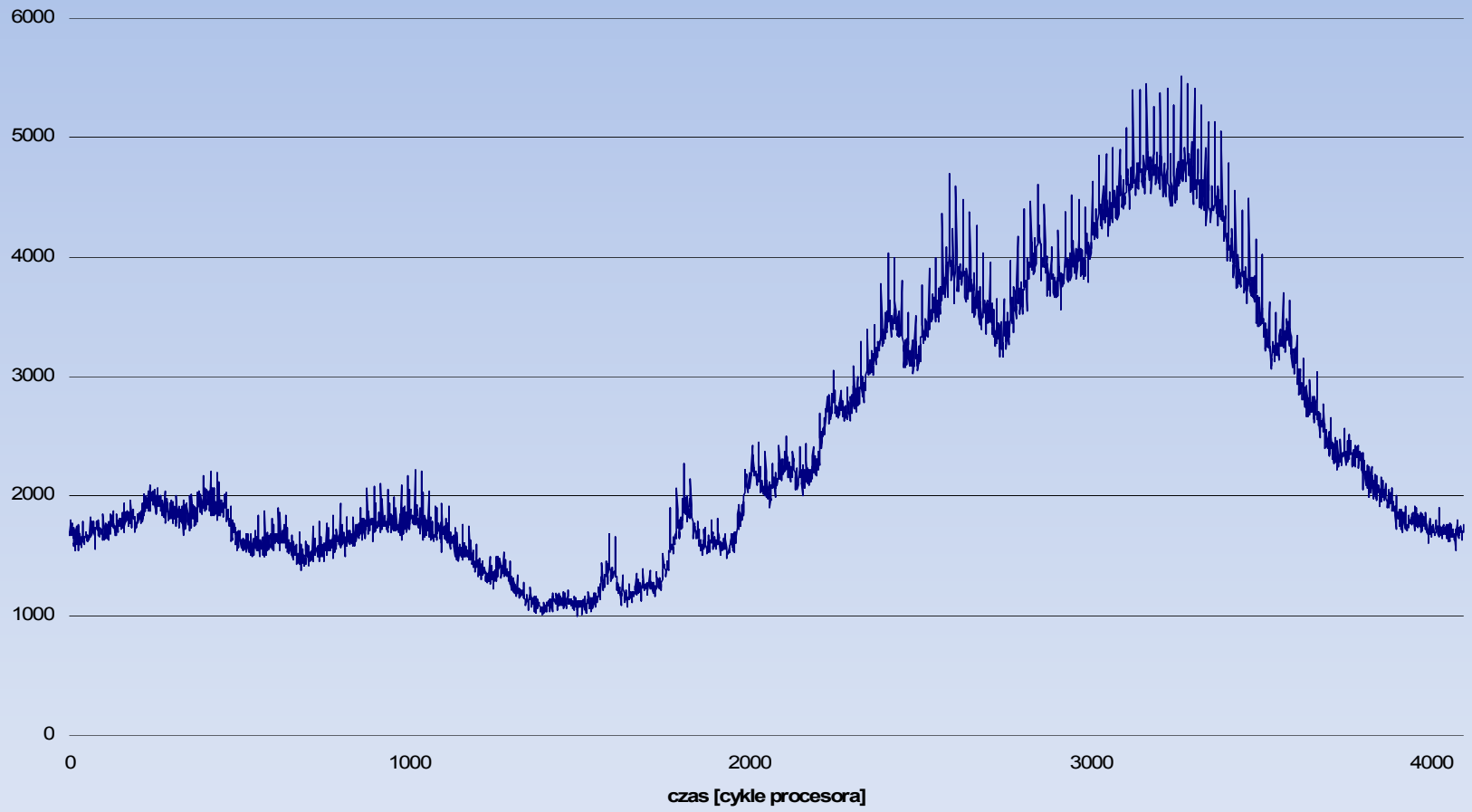
Analiza dysku twardego jako źródła entropii

- Zasada pozyskiwania entropii
  - Zapisujemy na dysk twardy blok danych o określonym rozmiarze.
  - Turbulencje powietrza w napędzie dyskowym, drgania głowicy czy losowość zawarta w samym systemie operacyjnym powodują pewne odchylenia od wartości oczekiwanej.
  - Dwa tryby zapisu
    - write-through – natychmiastowy bloku danych na dysk
    - write-back – najpierw dane zapisywane do pamięci podręcznej następnie na dysk

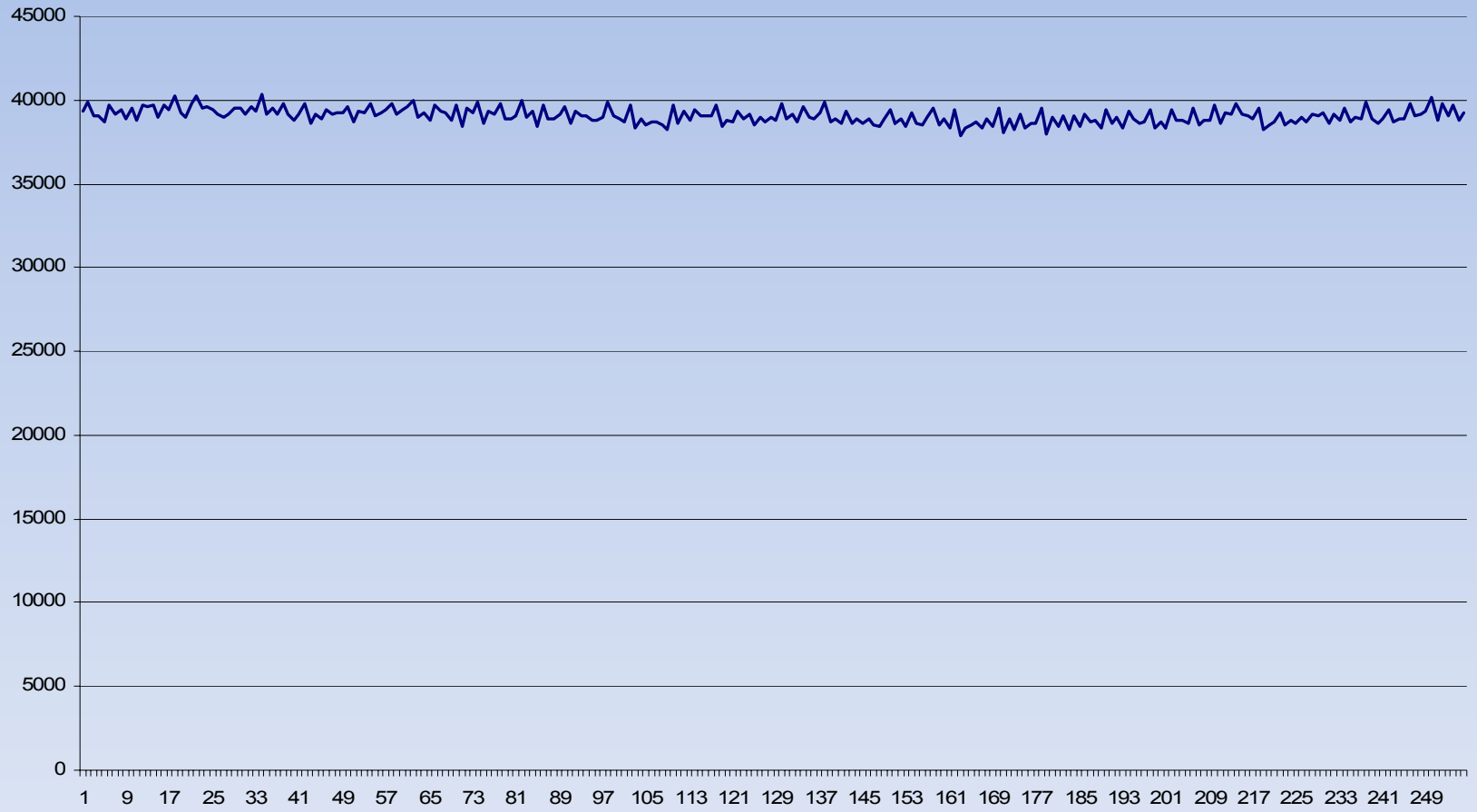
Czas zapisu (najmłodsze 16 bitów) 1000 bajtowego bloku danych mierzony w taktach procesora



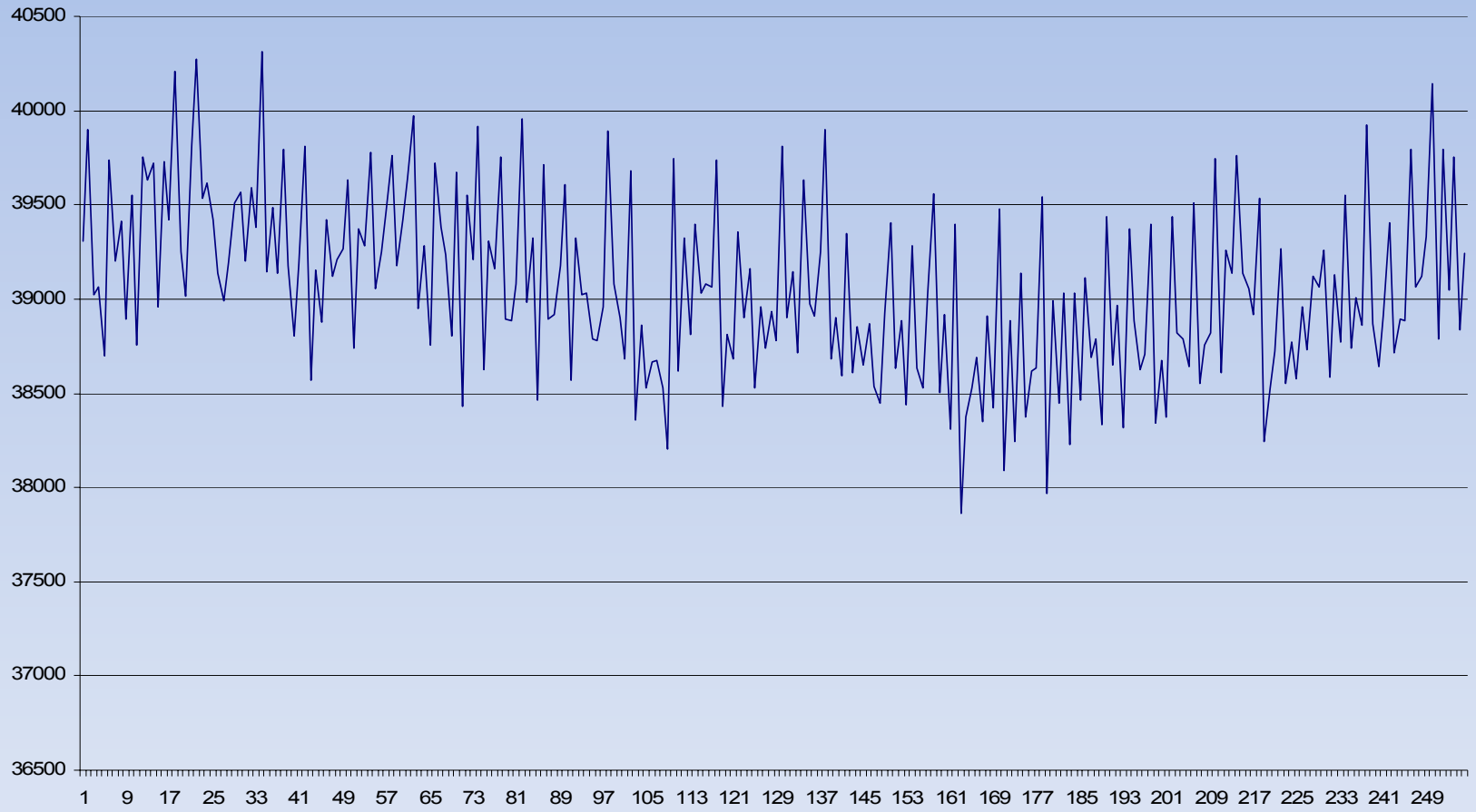
Czas zapisu (najmłodsze 12 bitów) 1000 bajtowego bloku danych mierzony w taktach procesora



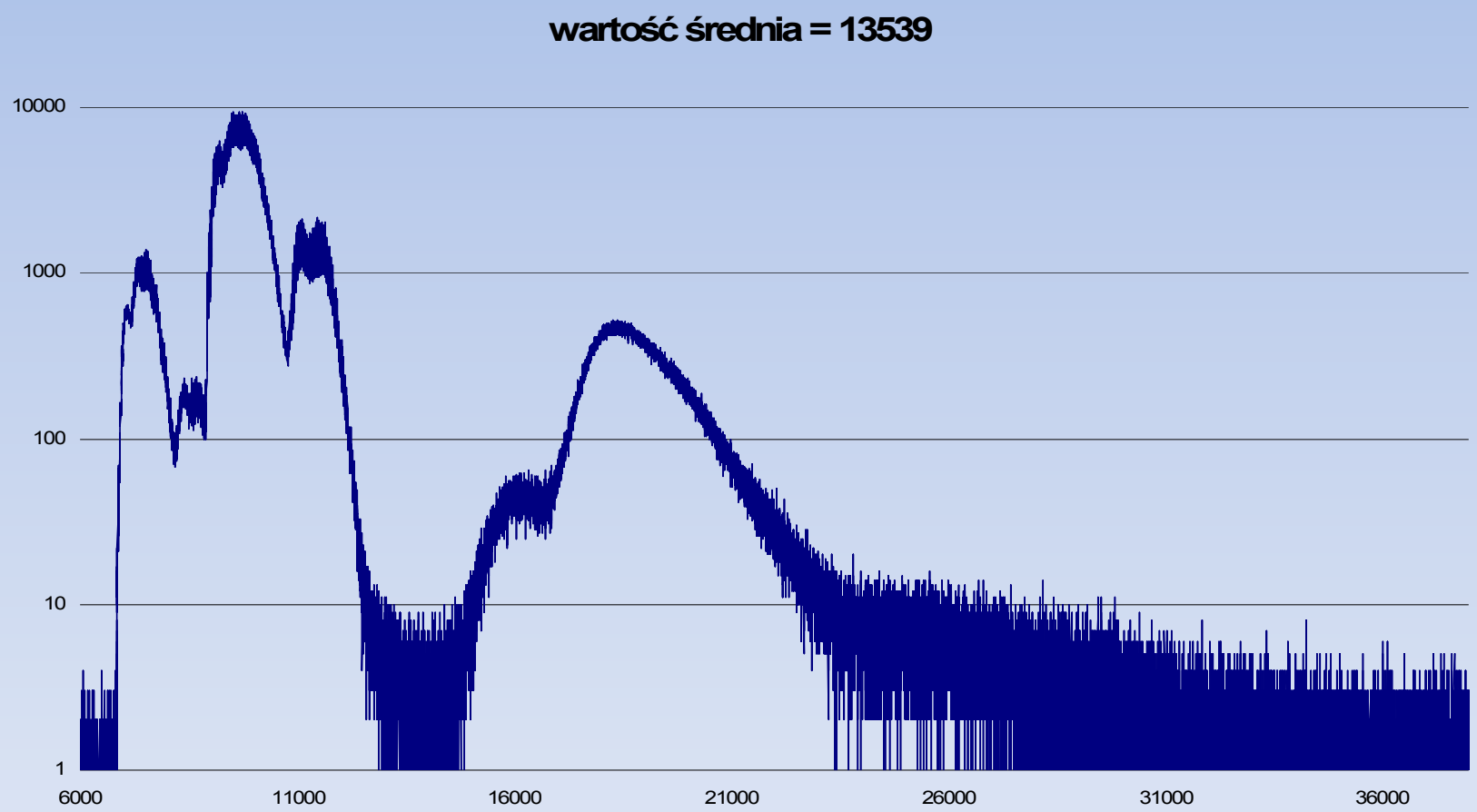
Czas zapisu (najmłodsze 8 bitów) 1000 bajtowego bloku danych mierzony w taktach procesora



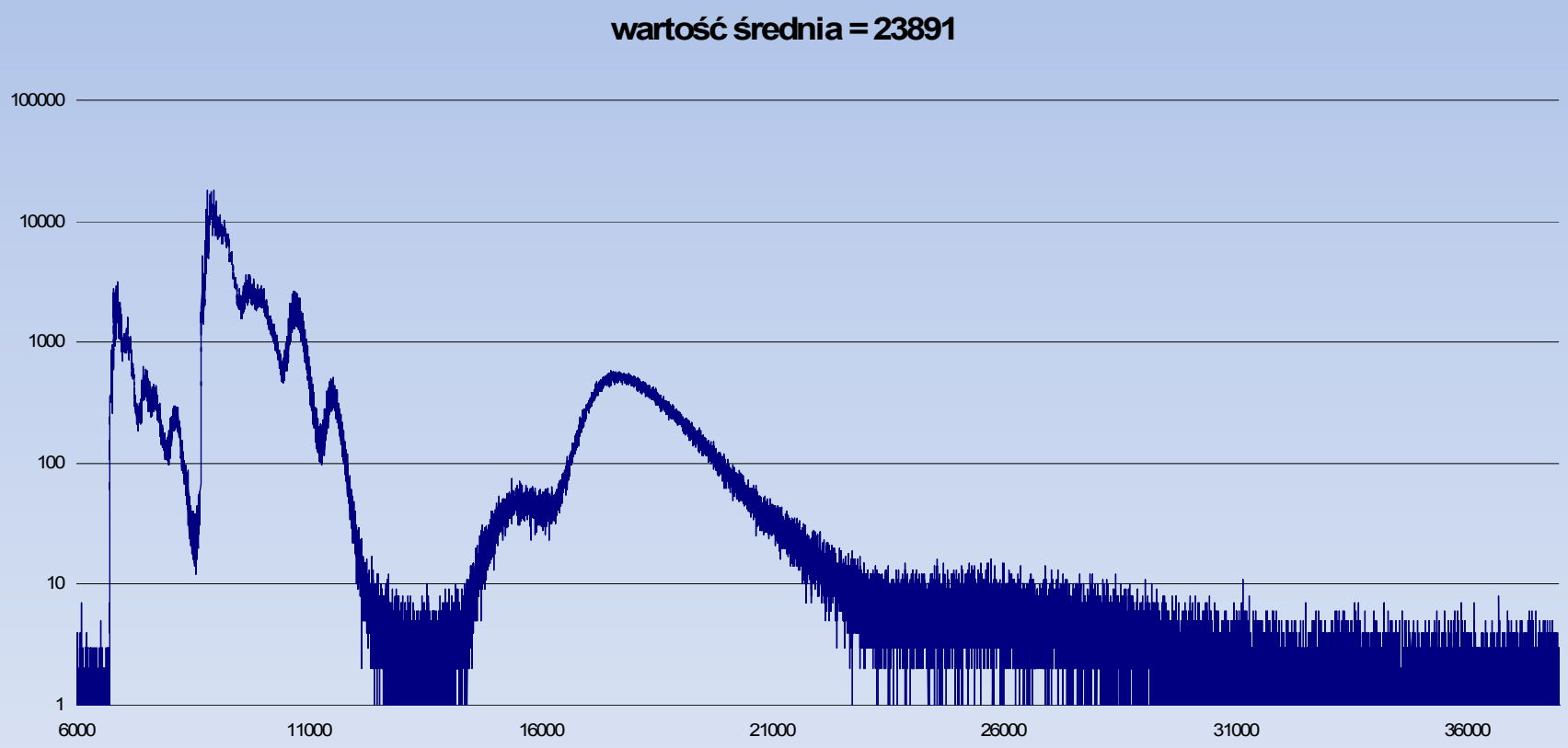
Czas zapisu (najmłodsze 8 bitów) 1000 bajtowego bloku danych mierzony w taktach procesora



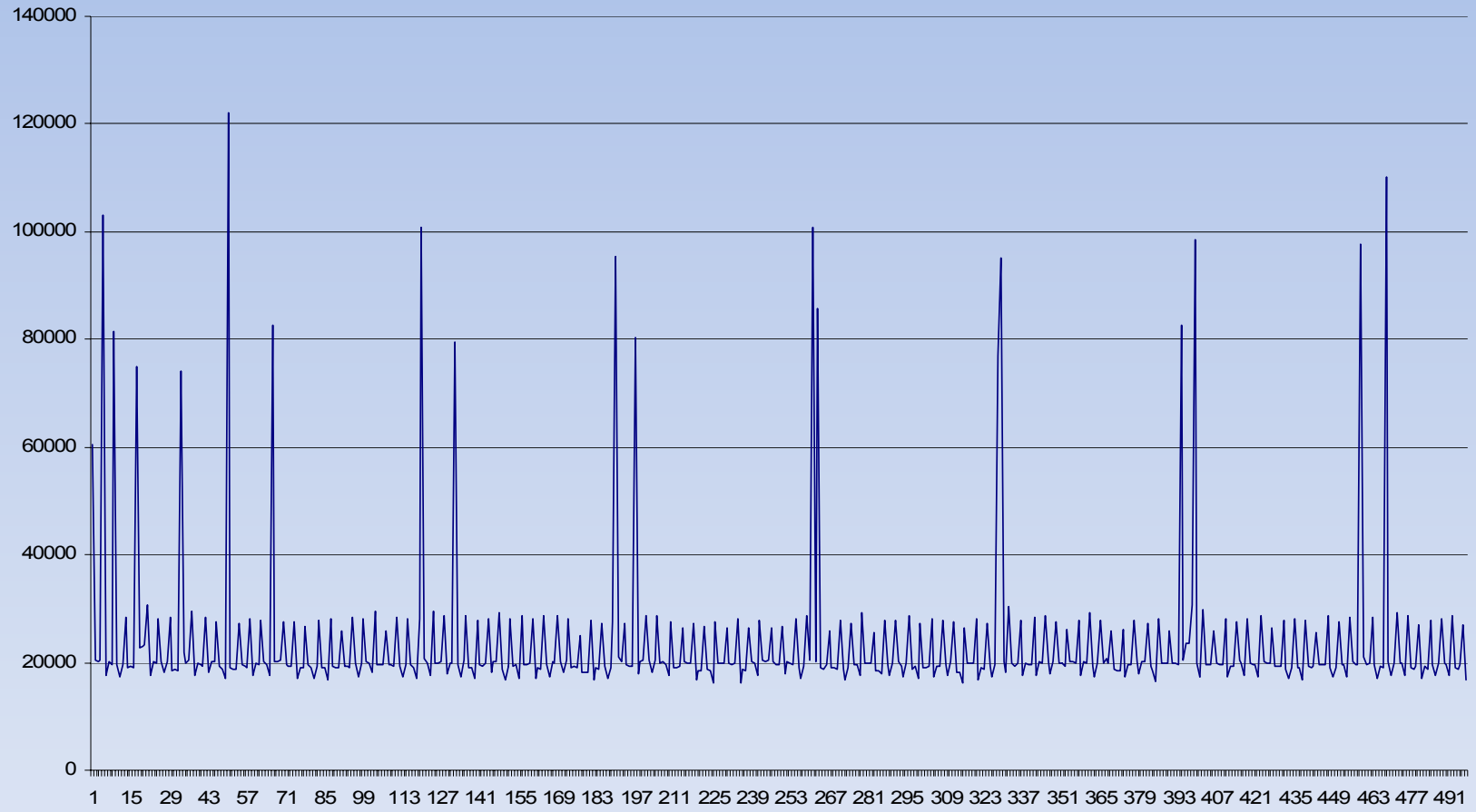
Czas zapisu (najmłodsze 16 bitów) 500 bajtowego bloku danych mierzony w taktach procesora Dysk nieobciążony



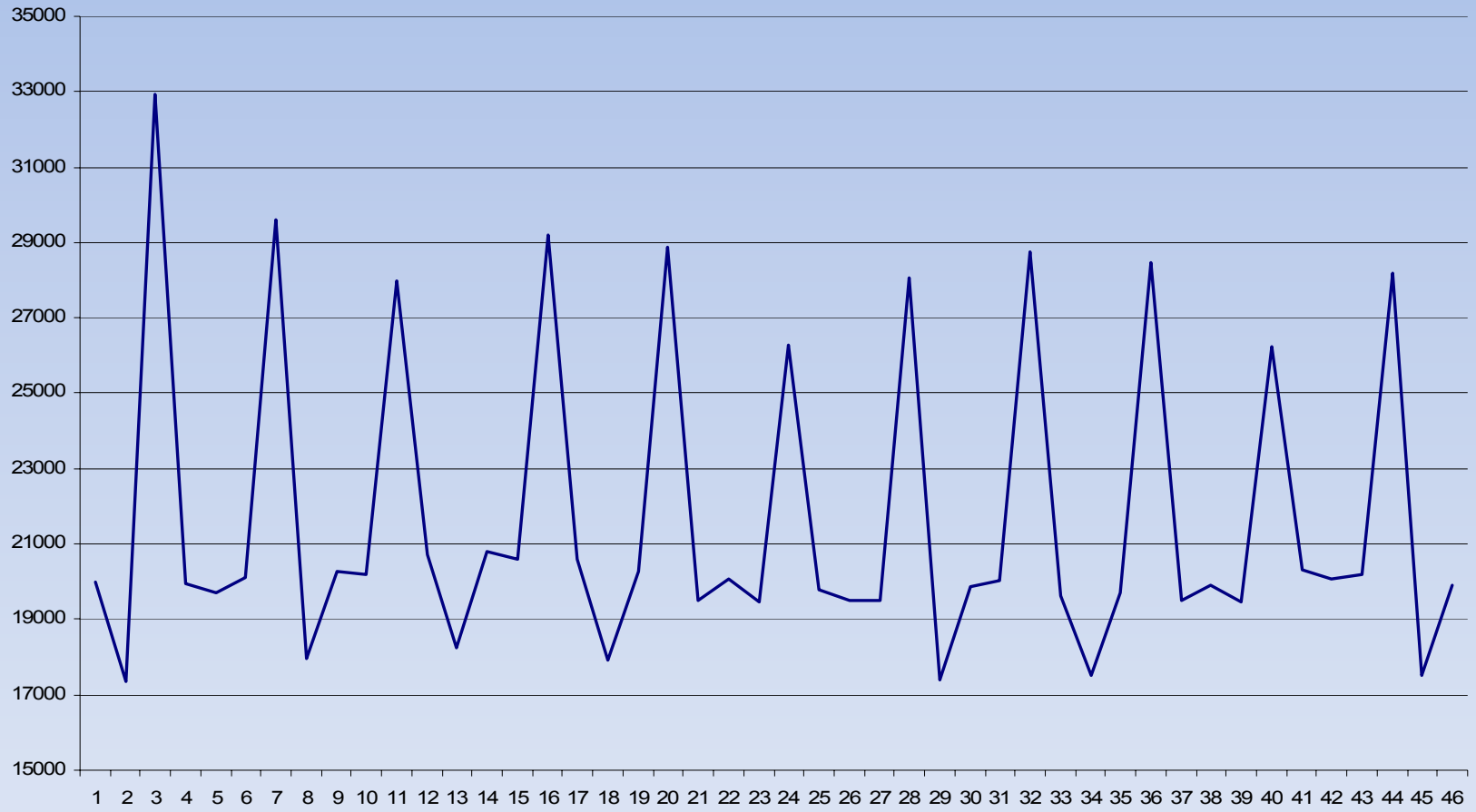
Czas zapisu (najmłodsze 16 bitów) 500 bajtowego bloku danych mierzony w taktach procesora
Dysk obciążony 2MB/s



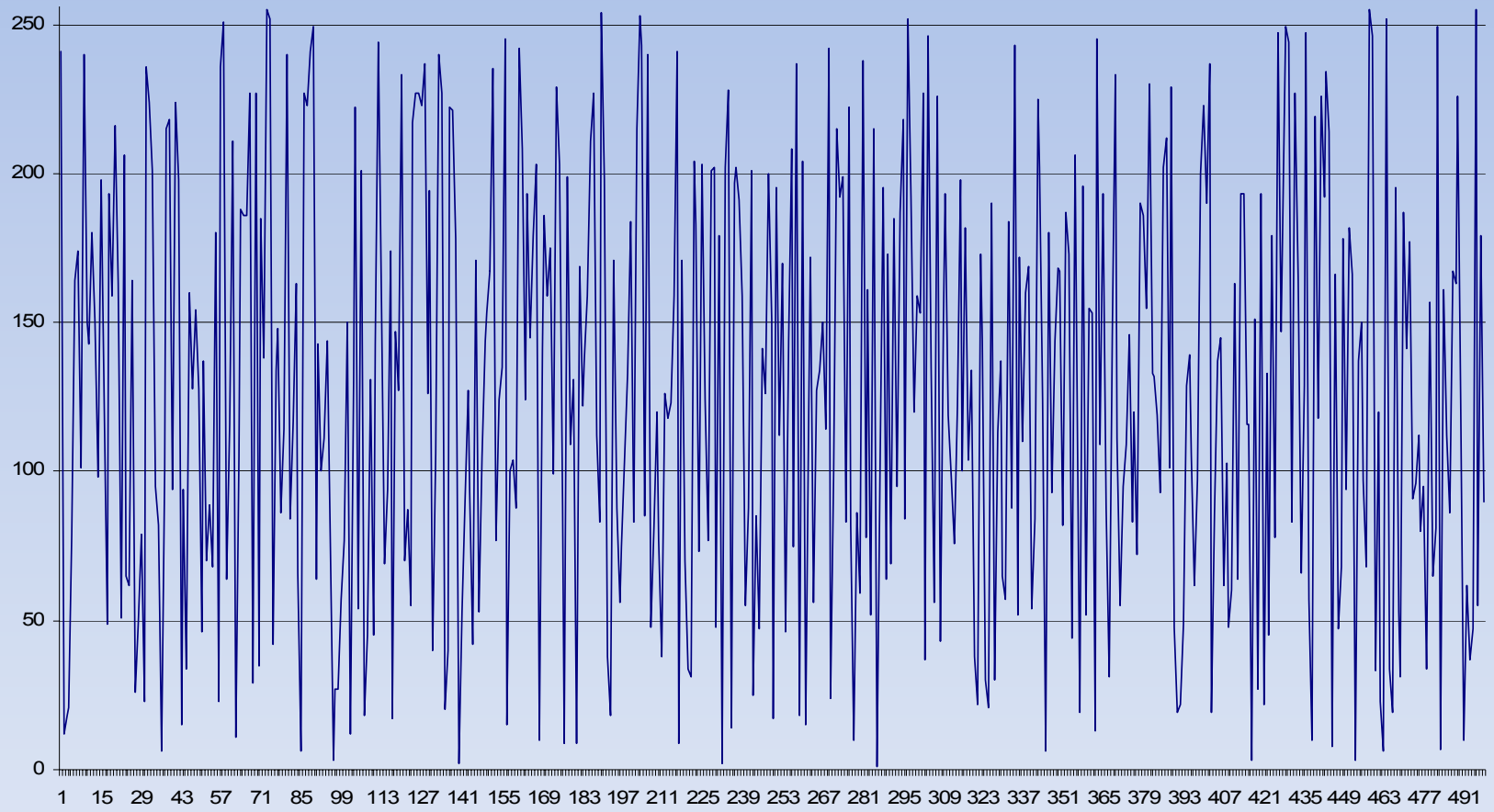
Korelacja próbek



Korelacja próbek



Korelacja kolejnych wartości modulo 256



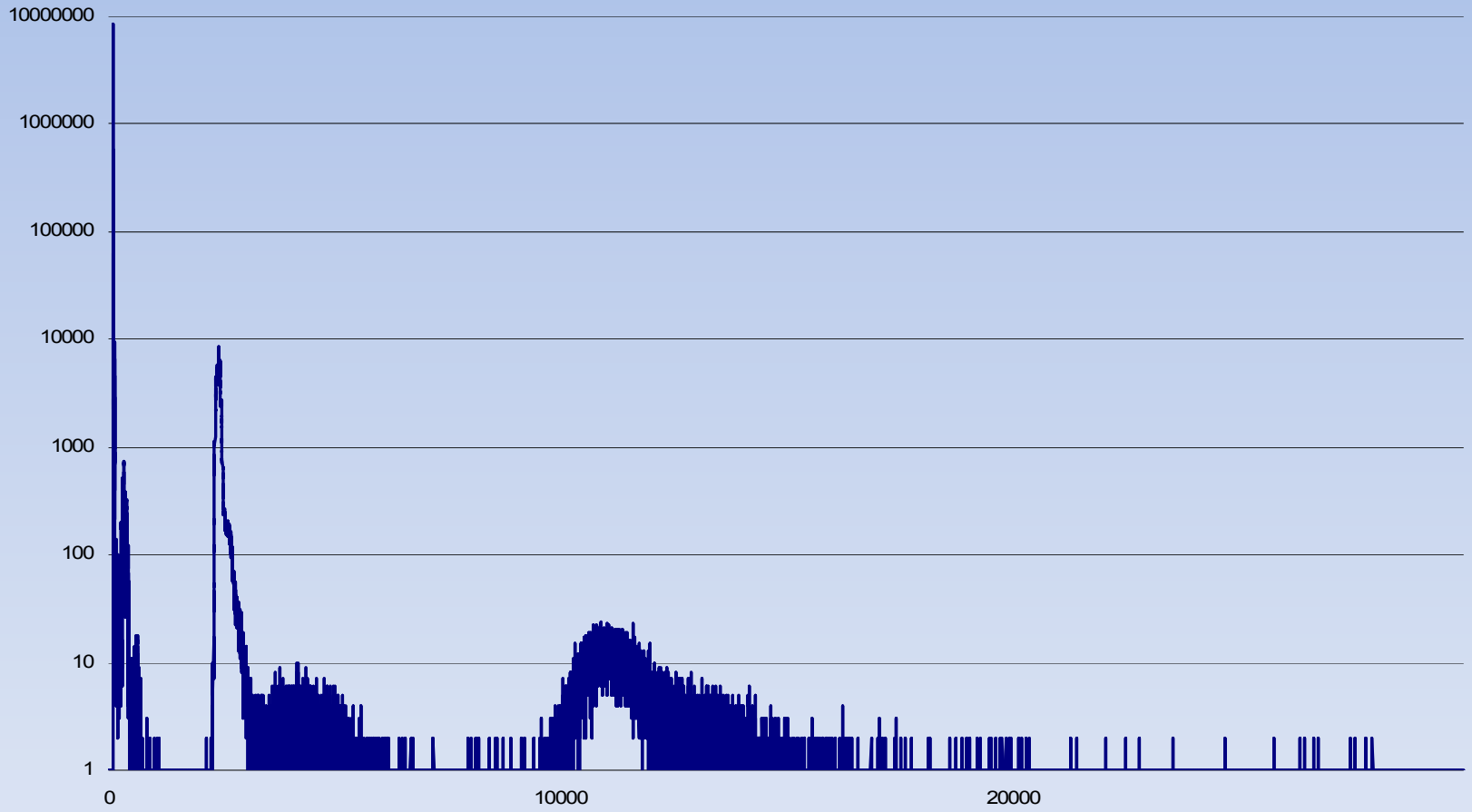
Kontrola losowości bitów

- kompresja bezstratna
  - Ciąg losowy nie zawiera nadmiarowości.
- testy statystyczne
  - DIEHARD
  - Crypt-XS
  - NIST Statistical Test Suite

Szybkość źródła

- Dla bloku 1000 bajtów
  - Średni czas zapisu 34000 cykli zegara ok. 20µs
  - 8 bitów na 20µs => 400 Kb / s
- Dla bloku danych 160 bajtów
  - Średni czas zapisu 6400 cykli zegara
  - 6 bitów 4µs => 1,5 Mb/s

Zbyt mała długość bloku danych



Kalibracja generatora

- Dobór rozmiaru bloku zapisywanego na dysk w zależności od szybkości dysku
- Podatne na manipulację
  - Obciążenie dysku przez napastnika podczas kalibracji spowoduje wybranie zbyt krótkiego bloku danych
- Kalibracja ‘online’
  - Wyliczając z N poprzednich próbek średni czas zapisu zmieniamy rozmiar bloku danych.

Testy źródła entropii

- Test źródła entropii ma na celu sprawdzanie czy źródło generuje bity z niezerową entropią
- Test jest w stanie wykryć jedynie awarię źródła.
- Najbardziej skomplikowane testy nie są w stanie wykryć przejęcia kontroli nad źródłem przez napastnika

Wybór funkcji przejścia

- Pozbycie się wzajemnej korelacji próbek
  - Przeplot
  - Szyfrowanie algorytmami symetrycznymi

Funkcja generująca wyjście

- Jednokierunkowa funkcja skrótu
  - Oddziaływanie na bity losowe jednokierunkową funkcją skrótu powiększa entropię w stosunku do entropii wejściowej
  - Jeżeli na wejściu j.f.s. podamy ciąg bitów którego łączna entropia jest większa od rozmiaru wyjściowego ciągu bitów j.f.s, to entropia każdego z wyjściowych bitów będzie równa 1

Test generatora

- sprawdzenie czy generowane bity rzeczywiście są losowe
  - kompresja bezstratna
  - testy statystyczne
    - DIEHARD
    - Crypt-XS
    - NIST Statistical Test Suite

Dziękuje za uwagę