Kryptografia postkwantowa

Mikołaj Koszowski 274392
Hubert Nowakowski 274415

Zad7. wariant 5
Kod źródłowy: github.com/Fisher16/KiBD

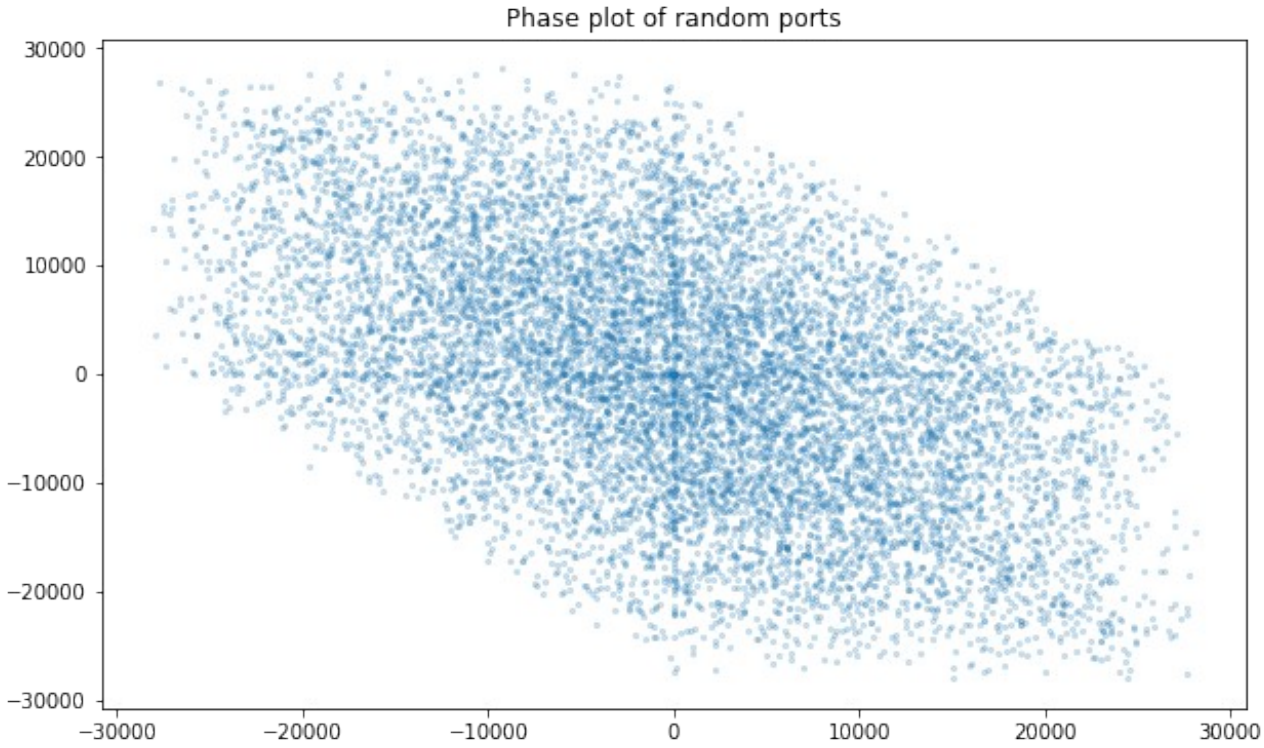
Połączenie TCP jest zapoczątkowane przez tak zwany *3-way handshake*. Klient wysyła pakiet SYN (*Synchronize*) następnie serwer odsyła SYN/ACK na co klient odpowiada pakietem ACK (*Acknowledgement*). W celu zapewnienia bezpieczeństwa wymieniana jest między nimi 4 bajtowa losowa sekwencja liczbowa służąca do weryfikacji kolejności przepływu informacji.[1] Ponadto w celu zwiększenia możliwej liczby unikalnych połączeń między klientem a serwerem, losowany jest 2 bajtowy numer portu identyfikujący dane połączenie.

Stworzyliśmy program do podsłuchiwania ruchu (*sinffer*), który filtruje pakiety SYN i wyciąga z nich te dwa losowe pola, a następnie wypisuje je na standardowe wyjście, wykorzystaliśmy do tego bibliotekę **scapy**. Następnie wykorzystaliśmy crawler napisany w frameworku **scrapy** w celu wykonania sporej ilości zapytań do różnych serwerów. Zebraliśmy ponad **10k** losowych pól kolejnych pakietów SYN.

Analogicznie do metod zastosowanych przez Michała Zalewskiego (*Strange Attractors and TCP/IP Sequence Number Analysis*) [2] wykonaliśmy portrety fazowe, stosując rozwinięcie Takensa.

Co do początkowych sekwencji nie zauważyliśmy występowania atraktorów, co przedstawia poniższy wykres:

Natomiast w przypadku pól związanych z numerem portu zauważyliśmy występowanie zagęszczenia w pobliżu wartości zero jak i na przekątnej, krzyż widoczny poniżej:



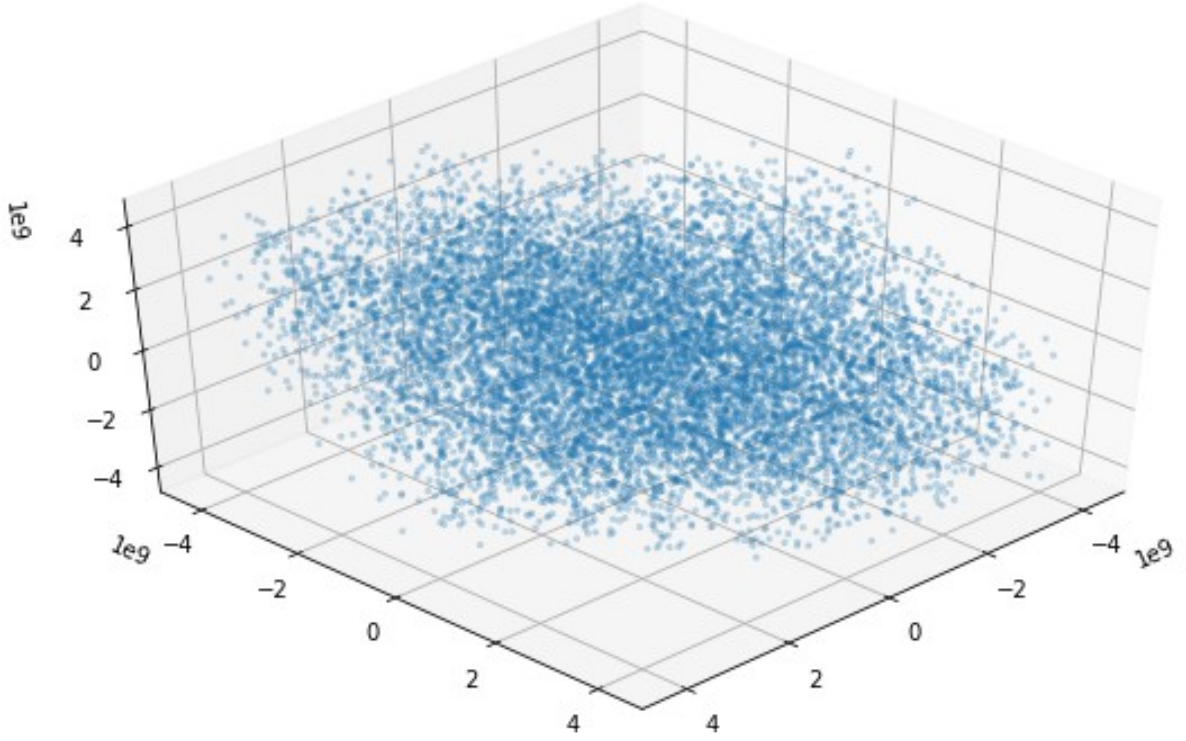
Wynika to z występowania różniących się o wartość 2 kolejnych wartości portu. Zauważyliśmy że powstają one przy kolejnych połączeniach do tej samej strony/serwera.

Stosowane rozwinięcie:
x[n] = s[n-2] - s[n-3]
y[n] = s[n-1] - s[n-2]
z[n] = s[n] - s [n-1]

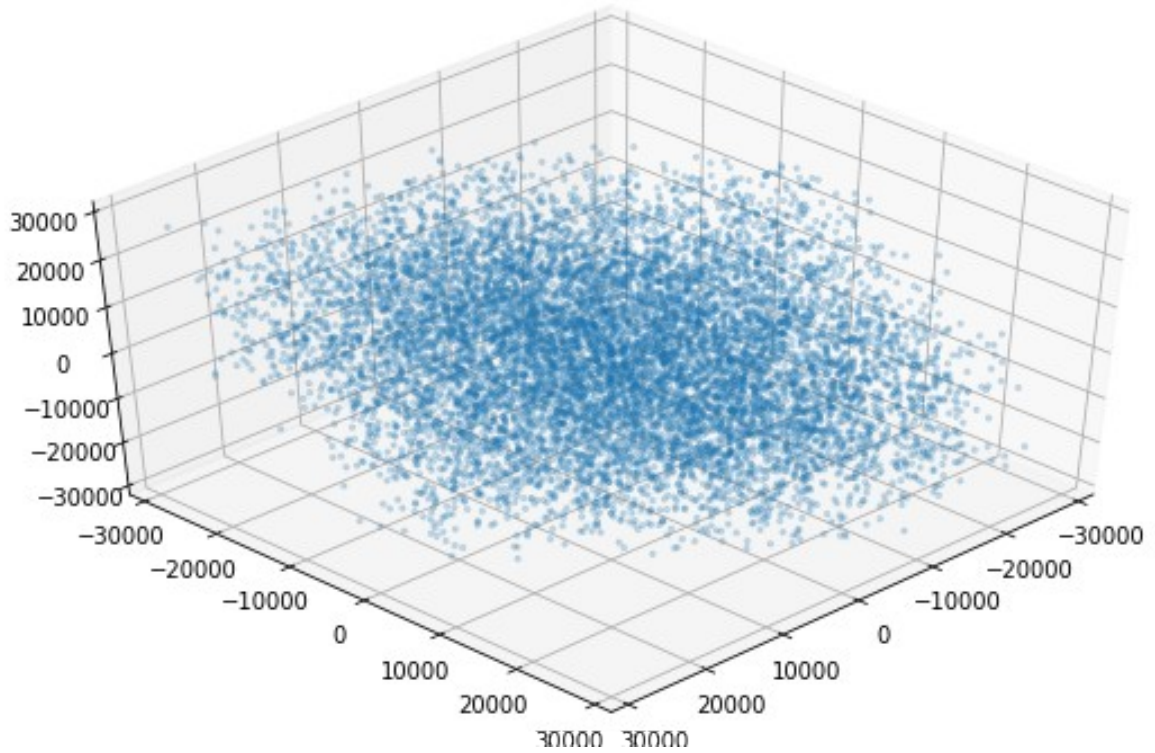
Powyższe wykresy dla punktów (Y,Z). W celu wytłumaczenia obserwowanego krzyża rozważmy trzy kolejne wartości; a,b,c.

$a \approx b \approx c \rightarrow (y,z) = (0,0)$
$a \approx b, rand\, c \rightarrow (y,z) = (0, c-b)$
$rand\, a, b \approx c \rightarrow (y,z) = (b-a, 0)$
$a \approx c, rand\, b \rightarrow (y,z) = ((b-const), -(b-const)) \rightarrow y = -z$

Dołączamy również rzut w 3D:
Przestrzeń fazowa początkowych sekwencji:



Przestrzeń fazowa wylosowanych portów:



Źródła:
[1] https://packetlife.net/blog/2010/jun/7/understanding-tcp-sequence-acknowledgment-numbers/
[2] https://lcamtuf.coredump.cx/oldtcp/tcpseq.html
Zobrazowanie potrzeby wizualizacji portretu fazowego w 3D:
https://www.reddit.com/r/dataisbeautiful/comments/gv4fhr/oc_why_randu_is_a_bad_random_number_generator/