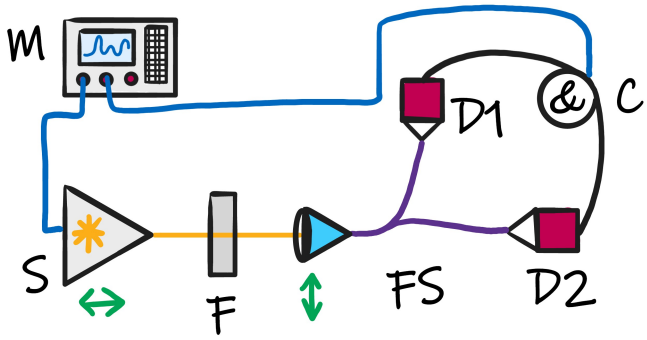
Marta Misiaszek - Schreyner

Elementy systemu kwantowego generatora liczb losowych

17 października 2022

Kwantowy generator liczb losowych (z ang. Quantum Random Number Generator (**QRNG**)) jest urządzeniem dostarczającym wysokiej jakości entropię. Entropia, lub inaczej mówiąc losowość, jest jednym z kluczowych elementów dzisiejszych systemów kryptograficznych, w szczególności korzystających z losowo wybranych kluczy kryptograficznych do kodowania i transmisji danych.

Entropia generowana przez QRNG, której pochodzenie związane jest ściśle z fizycznymi prawami rządzącymi materią (mechaniką kwantową), jest najlepszej możliwej jakości, jaką obecnie możemy oczekiwać. Istnieją różne sposoby generowania takiej entropii, jednym z nich jest odpowiednia detekcja fotonów.



Rysunek 1: *Schemat ideowy kwantowego generatora liczb losowych.*
Symbole: S – źródło światła, F – filtr osłabiający, FS – światłowodowy dzielnik wiązki, D1,D2 – detektor, C – korelator, M – system sterujący.
Zielone strzałki symbolizują kierunek, w którym położenie elementów może być sterowane.

Schemat zaprojektowanego przez *Quantum Blockchains* generatora zaprezentowany jest na Rysunku 1. Składa się on z następujących elementów:

→ *źródło światła (S)* – dioda lub laser diodowy, którego intensywność (prąd/napięcie) i położenie w przestrzeni (przesunięcie ok. 10 mm) może być sterowane;

→ *osłabiacz wiązki (F)* – nieruchoma płytka osłabiająca intensywność źródła światła;

→ *światłowodowy dzielnik wiązki (FS)* – światłowodowy dzielnik wiązki (położenie regulowane prostopadle do kierunku wiązki, ok. 5mm) ;

→ *detektory (D1, D2)* – fotodiody lawinowe (SPAD), rejestrujące sygnały ze źródła światła;

→ *korelator (C)* – korelator sygnałów przychodzących z detektorów;

→ *system sterujący (M)* – oparty o kartę FPGA, sterujący położeniem źródła światła, jego intensywnością oraz dobierający odpowiednie parametry po przeanalizowaniu danych otrzymanych z korelatora sygnałów.

Jak widzimy na Rysunku 1, wiązka fotonów generowana przez źródło (S) jest osłabiana za pomocą filtra (F) do poziomu pojedynczych fotonów. Pojedynczy foton skupiany jest do światłowodowego dzielnika wiązki (FS), a następnie zgodnie z zasadami mechaniki kwantowej ma 50% szans na opuszczenie go jednym lub drugim wyjściem. Następnie foton jest rejestrowany przez któryś z detektorów (D1 lub D2). Sygnał z detektorów trafia do korelatora (C), gdzie podlega sprawdzeniu. Informacja o nim jest następnie przesyłana do systemu sterującego (M), gdzie dobierane są odpowiednie parametry dla źródła światła.

Jakość entropii generowanej przez prezentowany układ zależy od kilku czynników. Najważniejszym elementem jest źródło światła. Zakładamy tu użycie diody lub lasera diodowego, którego intensywność może być regulowana za pomocą zmiany napięcia tak, aby przy detekcji uzyskiwać średnio jeden foton w danym oknie. Istotne jest zatem również badanie korelacji sygnałów pochodzących z detektorów, gdyż rejestracja sygnału na obu detektorach jednocześnie oznacza, że należy zmniejszyć intensywność źródła. Kolejnym niezwykle istotnym elementem jest system sterujący, przetwarzający informację z korelatora i sterujący elementami mechanicznymi. Szybkie dostrajanie parametrów źródła pozwoli na szybszą generację lepszej jakościowo entropii.

Zaprezentowany na Rysunku 1 układ powinien zatem mieć możliwość pracy w dwóch schematach – **testowej** (gdzie sprawdzana będzie jakość generowanej entropii) oraz **generującej** (gdzie na wyjściu podawane będą konkretne bity 0 lub 1). W idealnym przypadku testowy mod pracy mógłby być prowadzony w czasie rzeczywistym, nie jest to jednak konieczne.

Przewiduje się, że jakość entropii będzie sprawdzana w następujących (lub podobnych) krokach:

1. Ustaw parametry źródła S. Wygeneruj wiązkę fotonów.
2. Ustaw położenie dzielnika wiązki.
3. Wykonaj pomiar koincydencyjny oraz zbierz sygnały z detektorów D1 i D2 w określonym czasie (wartości *kliknięć* z obu detektorów oraz *kliknięć* jednoczesnych).
4. Wykonaj obliczenie funkcji korelacji.
5. Jeżeli wartość jest wyższa niż oczekiwana, zmniejsz intensywność lasera (lub zmień jego położenie), jeżeli jest właściwa nie rób nic.
6. Wykonaj wszystkie punkty instrukcji ponownie.

Warto zauważyć, że zaprojektowany tak QRNG jest samotestujący i samoustawiający się, co oznacza, że użytkownik samodzielnie jest w stanie wygenerować entropię, bez korzystania z zewnętrznych serwisów, a jej jakość monitorować w czasie rzeczywistym.