System i sposób generowania symetrycznego klucza kryptograficznego oraz liczb losowych

Przedmiotem wynalazku jest system i sposób generowania symetrycznego klucza kryptograficznego oraz liczb losowych, mający swoje zastosowanie do wykonywania czynności kryptograficznych w celu zapewnienia bezpieczeństwa komunikacji w infrastrukturze publicznej.

Standardowa kryptografia, a w szczególności dystrybucja klucza kryptograficznego stoi wobec wyzwania ze strony komputerów kwantowych, których wykorzystanie stanowi zagrożenie dla asymetrycznych algorytmów kryptograficznych, takich jak powszechnie używany w Internecie kryptosystem RSA.

Według przewidywań, komputery kwantowe staną się dostępne w ciągu 10 lat, jednakże, aby zachować bezpieczeństwo sposób szyfrowania informacji należy zmienić już teraz, tym bardziej, że aktualna komunikacja może być zapisana obecnie, a odczytana wtedy, gdy komputery kwantowe staną się powszechnie osiągalne.

Na dziś, dostępne są dwie opcje: kryptografia kwantowa i post-kwantowa. Ta druga to zestaw algorytmów działających na klasycznym hardware, w których przypadku algorytm Shora nie może zostać efektywnie zastosowany. Ze względu na niewielką ilość przeprowadzonych badań trudno jest oszacować czy inne algorytmy kwantowe lub klasyczne mogą zostać użyte do ich złamania.

Kryptografia kwantowa, z kolei, podatna jest na ataki wykorzystujące niedoskonałą implementację urządzeń. Na szczególną uwagę zasługują ataki oślepiające detektory detector blinding attacks, które wykorzystują fakt, że duża część fotonów użytych do komunikacji nie zostaje zarejestrowana przez

odbiorniki. Tego typu ataki zostały z powodzeniem wykorzystane przeciw większości komercyjnie dostępnych systemów.

Problemy stojące przed kryptografią kwantową wydają się poważniejsze niż te, z którymi mierzy się post-kwantowa, dlatego amerykańska NSA, francuska ANSSI oraz brytyjskie NCSC wydały rekomendacje, aby to ta druga opcja była w przyszłości używana źródło: www.nsa.gov, www.ssi.gouv.fr, www.ncsc.gov.uk.

Rozwiązaniem, które uczyniłoby kryptografię kwantową bardziej bezpieczną od post-kwantowej jest jej bardziej zaawansowana wersja, nazwana kryptografią niezależną od urządzeń device independent cryptography. Bezpieczeństwo klucza gwarantowane w niej jest przez rozkład prawdopodobieństwa otrzymywanych wyników i nie zależy w ogóle od tego jakie urządzenie je wygenerowało. Sprawia to, że wszystkie ataki wykorzystujące niedoskonałą implementację nie są skuteczne.

Niestety, bardzo trudno jest zbudować urządzenia pozwalające otrzymać rozkład prawdopodobieństwa gwarantujący bezpieczeństwo. Największą trudnością jest uzyskanie dużej efektywności detekcji fotonów. Dlatego też pierwsze eksperymentalne demonstracje tego typu kryptografii zostały wykonane dopiero w 2021 roku, a odległość pomiędzy komunikującymi się stronami nie przekraczała kilkuset metrów, źródło: https://arxiv.org/abs/2110.00575.

Tym, co pomogłoby uczynić kryptografię kwantową niezależną od urządzeń, bardziej bezpieczną, tańszą i dać jej większy zasięg, innymi słowy – uczynić bardziej praktyczną – jest opracowanie systemów o niższych wymaganiach odnośnie do prawdopodobieństwa detekcji fotonów.

System kryptografii niezależnej od urządzeń musi składać się z przynajmniej dwóch urządzeń, które łamią jakąś z nierówności Bella, za: A. Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett., 67, 661 1991.

Dla takich nierówności jednym z najważniejszych parametrów jest graniczna wartość efektywności detekcji fotonów, nazywana efektywnością krytyczną. Urządzenia wykrywające fotony z efektywnością niższą od krytycznej dla konkretnej nierówności Bella nie są w stanie łamać tej nierówności i przez to nie mogą zostać użyte w protokole dystrybucji klucza o nią opartym.

Aby ustalić efektywność urządzeń wykorzystywanych w konkretnym systemie kryptograficznym należy zsumować wszystkie straty fotonów od momentu ich wytworzenia w źródle do zarejestrowania w detektorze. Dlatego, im dłuższa odległość pomiędzy elementami systemu, a co za tym idzie – większe straty podczas ich przesyłania, tym mniejsza jest obserwowana efektywność i tym trudniej złamać jest nierówność Bella. Powyższe, skutkuje tym, że, wysoka wartość krytycznej efektywności przekłada się na małą maksymalną odległość pomiędzy elementami systemu, co czyni większość proponowanych do tej pory rozwiązań niepraktycznymi.

Dla systemów opartych o pary splątanych kubitów najlepsze znane nierówności Bella mają krytyczną efektywność wynoszącą 83%, jeśli stany są maksymalnie splątane lub wynoszącą 67% dla stanów bliskich produktowemu. Obie wartości są bardzo trudne do zrealizowania w praktyce.

Każdy system wykorzystujący łamanie nierówności Bella do generacji klucza kryptograficznego produkuje liczby losowe w urządzeniach wytwarzających klucz, dlatego może zostać też wykorzystany jako generator losowości.

Podobnie jak w przypadku tworzenia klucza kryptograficznego, taki generator liczb losowych będzie w stanie produkować liczby o niezerowej entropii wyłącznie, jeśli detekcja fotonów przekroczy wartość krytyczną.

Pomysł wykorzystania kwantowej nielokalności do generacji klucza kryptograficznego pojawił się w wielu publikacjach, jednak rozwiązania w żadnej

z nich nie pozwalają na poprawne działanie urządzenia przy niskiej efektywności detektorów.

W stanie techniki znany jest chiński wynalazek o nr CN 108984153, opisujący system i metodę niezależnego od urządzenia kwantowego generatora liczb losowych, zawierający źródło splątania, stację pomiarową Alicja, stację pomiarową Bob, centrum przetwarzania danych i źródło sygnału synchronicznego. W celu skutecznego działania, rozwiązanie to wymaga 78% efektywności detektorów.

Z kolei, inny chiński wynalazek o nr WO 2019125733, ujawniający wzmacnianie, generowanie lub poświadczanie losowości oraz amerykański wynalazek o nr US 9471280, dotyczący sposobu generowania losowego ciągu bitów pozwalają na użycie dowolnej nierówności Bella, przez co odnoszą się do nich znane do tej pory wszystkie ograniczenia dotyczące nierówności.

W stanie techniki znane są także rozwiązania, które wymagają uczciwego próbkowania fair sampling. Przyjmuje się w nich, że wszystkie niedoskonałości detektorów nie wynikają z hakerskich ataków na system. W efekcie takiego założenia zmniejsza się bezpieczeństwo protokołu kryptograficznego do poziomu standardowej kryptografii kwantowej. Przykładem takiego rozwiązania może być opisany w amerykańskim wynalazku o nr US 7428562, ujawniający generator kwantowych liczb losowych.

Niekorzystnymi cechami znanych do tej pory rozwiązań dotyczących generowania klucza kryptograficznego jest niewielki zasięg urządzeń, mała odporność na szumy w kanałach komunikacyjnych oraz bardzo wysokie wymagania odnośnie do efektywności detekcji fotonów.

Celem wynalazku jest eliminacja tych niedogodności.

Istotą wynalazku jest system generowania symetrycznego klucza kryptograficznego oraz liczb losowych, stanowiący układ urządzeń nadawczych,

odbiorczych oraz pomiarowych, charakteryzujący się tym, że tworzony jest przez zespół centralny, zespół pośredniczący oraz użytkownika końcowego, przy czym zespół centralny zawiera wyposażony w procesor główny nadajnik centralny oraz generujące stany kwantowe źródło splątania, połączone z przesyłającym stany kwantowe przekaźnikiem sygnałów, który wraz z powiązanym z nim, posiadającym funkcjonalność mierzenia stanów kwantowych urządzeniem pomiarowym, a także koprocesorem tworzy zespół pośredniczący, jednocześnie skomunikowany z procesorem głównym koprocesor odpowiedzialny jest za sterowanie przekaźnikiem sygnałów oraz urządzeniem pomiarowym, równocześnie przesyłający stany kwantowe przekaźnik sygnałów połączony jest ze zdolnym do mierzenia stanów kwantowych przyrządem pomiarowym, który razem, wraz z procesorem wchodzą w skład należącego do użytkownika końcowego odbiornika, przy czym procesor powiązany jest z procesorem głównym i odpowiada za komunikację z należącymi do innych użytkowników końcowych odbiornikami, równocześnie generowane przez źródło splątania stany kwantowe zawierają podsystemy, splątane w dowolnym stopniu swobody.

Korzystnie, podsystemy splątane są w polaryzacji.

Korzystnie, komunikacja w systemie odbywa się za pośrednictwem komunikacji przewodowej.

Korzystnie, komunikacja w systemie odbywa się za pośrednictwem komunikacji bezprzewodowej.

Istotą wynalazku jest także sposób generowania symetrycznego klucza kryptograficznego oraz liczb losowych, charakteryzujący się tym, że przekaźnik sygnałów łączy się z odbiornikiem i w procesorze generuje się zapisane w formie cyfrowej ciągi danych, które zawierają liczbę N oraz liczbę K, gdzie liczba N stanowi długość ciągów danych, następnie:

w przypadku generowania klucza kryptograficznego przeprowadza się, powtarzane N-krotnie poniższe czynności, tj.

– w procesorze, wchodzącym w skład odbiornika pierwszego użytkownika końcowego wybiera się losową liczbę naturalną *x* oraz liczbę binarną *i*, po czym obie liczby wysyła się do koprocesora, natomiast w procesorze, wchodzącym w skład odbiornika drugiego użytkownika końcowego wybiera się losową liczbę naturalną *y* oraz liczbę binarną *j*, po czym obie liczby wysyła się do koprocesora, z kolei

– w źródle splątania generuje się, będącą w stanie splątanym parę fotonów, którą wysyła się do przekaźników sygnałów, wchodzącego w skład pierwszego zespołu pośredniczącego oraz do przekaźnika sygnałów, wchodzącego w skład drugiego zespołu pośredniczącego, przy czym

– w pierwszym zespole pośredniczącym, jeśli liczba $i = 0$, to z przekaźnika sygnałów przesyła się stan kwantowy do urządzenia pomiarowego, w którym wykonuje się pomiar *x*, a otrzymany wynik pomiaru oznacza się jako *a* i odsyła się go poprzez koprocesor do procesora należącego do pierwszego użytkownika końcowego, natomiast jeśli liczba $i = 1$ to z przekaźnika sygnałów do odbiornika, należącego do pierwszego użytkownika końcowego przesyła się stan kwantowy, gdzie w jego przyrządzie pomiarowym wykonuje się pomiar *x*, analogicznie, w drugim zespole pośredniczącym, jeśli liczba $j = 0$, to z przekaźnika sygnałów przesyła się stan kwantowy do urządzenia pomiarowego, w którym wykonuje się pomiar *y*, a otrzymany wynik pomiaru oznacza się jako *b* i odsyła się go poprzez koprocesor do należącego do drugiego użytkownika końcowego procesora, natomiast jeśli liczba $j = 1$ to z przekaźnika sygnałów do odbiornika drugiego użytkownika końcowego przesyła się stan kwantowy, gdzie w jego przyrządzie pomiarowym wykonuje się pomiar *y*, po czym

– w odbiornikach należących do obu użytkowników końcowych generuje się ciągi liczb o długości N tak, że w odbiorniku pierwszego użytkownika końcowego dostępny jest ciąg liczb *x, i, a*, zaś w odbiorniku drugiego użytkownika końcowego dostępny jest ciąg liczb *y, j, b,* po czym dalej z powyższych ciągów liczb tworzy się klucz kryptograficzny, poprzez wykonanie następujących kroków:

– w procesorach obu użytkowników końcowych, z elementów ciągów liczb wybiera się losowo liczbę określającą dokładność oszacowania bezpieczeństwa klucza K, a za pomocą standardowych narzędzi statystycznych szacuje się rozkład prawdopodobieństwa *P(a, b, | x, y, i, j)*, natomiast, dla wszystkich pozostałych elementów w ciągach liczb: procesor pierwszego użytkownika końcowego przesyła do procesora drugiego użytkownika końcowego wartości *x, i*, zaś procesor drugiego użytkownika końcowego przesyła do procesora pierwszego użytkownika końcowego wartości *y, j,* po czym

– w procesorach obu użytkowników końcowych usuwa się z ciągów liczb wszystkie przypadki, z wyjątkiem tych kiedy $x = y$ *oraz* $i = j = 1$, po czym na podstawie *P(a, b | x, y, i, j)* w procesorach obu użytkowników końcowych oblicza się poziom korelacji pomiędzy pomiarami *a* oraz *b*, przy identycznych ustawieniach, czyli $E = P\ a = b \mid x = y,\ i = j = 1)$ oraz, także na podstawie *P(a, b | x, y, i, j)* w procesorach obu użytkowników końcowych oblicza się losowość wyników *a* oraz *b*, przy czym obliczenia wykonywane są za pomocą standardowej metody informatyki kwantowej, ponadto

– na wszystkich pozostałych elementach ciągów liczb w procesorach obu użytkowników końcowych wykonuje się korekcję błędów, przy czym na elementach ciągów liczb w procesorach obu użytkowników końcowych, przetworzonych podczas korekcji błędów wykonuje się amplifikację prywatności i generuje się wynik będący, symetrycznym kluczem współdzielonym przed odbiorniki obu użytkowników końcowych;

natomiast

w przypadku generowania liczb losowych przeprowadza się, powtarzane N-krotnie poniższe czynności:

– w procesorze użytkownika końcowego wybiera się losowo liczbę naturalną *x* oraz liczbę binarną *i*, po czym obie liczby wysyła się do koprocesora pierwszego zespołu pośredniczącego, z kolei

– w źródle splątania generuje się, będącą w stanie splątanym parę fotonów, którą wysyła się do odpowiednich przekaźników sygnałów obu zespołów pośredniczących, przy czym

– jeśli liczba *i = 0*, to z przekaźnika sygnałów pierwszego zespołu pośredniczącego przesyła się stan kwantowy do jego urządzenia pomiarowego, w którym wykonuje się pomiar *x*, a otrzymany wynik pomiaru oznacza się jako *a*, po czym odsyła się go poprzez koprocesor do procesora użytkownika końcowego, natomiast jeśli liczba i = 1 to z przekaźnika sygnałów pierwszego zespołu pośredniczącego do odbiornika użytkownika końcowego przesyła się stan kwantowy, gdzie w jego przyrządzie pomiarowym wykonuje się pomiar *x*, po czym otrzymany wynik pomiaru oznacza się jako *a*, a dalej

– koprocesor drugiego zespołu pośredniczącego wybiera losowo liczbę *y*, natomiast urządzenie pomiarowe pierwszego zespołu pośredniczącego wykonuje pomiar *y*, po czym otrzymany wynik pomiaru oznacza się jako *b*, w efekcie w odbiorniku użytkownika końcowego dostępny jest ciąg liczb *x, i, a*, zaś w drugim zespole pośredniczącym dostępny jest ciąg liczb *y, b*, następnie

– w odbiorniku użytkownika końcowego oraz w przekaźniku sygnałów drugiego zespołu pośredniczącego generuje się ciągi liczb o długości N tak, że w odbiorniku użytkownika końcowego dostępny jest ciąg *x, i, a* zaś w przekaźniku sygnałów drugiego zespołu pośredniczącego dostępny jest ciąg *y, b, a*, po czym

– w procesorze użytkownika końcowego z elementów jego ciągu liczb *x, i ,a* wybiera się losowo mniejszą od liczby N liczbę K, po czym z odbiornika użytkownika końcowego wysyła się do przekaźnika sygnałów drugiego zespołu pośredniczącego żądanie przesłania odpowiadających ciągowi danych *x, i, a* odpowiednich elementów, następnie na podstawie wysłanych przez przekaźnik sygnałów drugiego zespołu pośredniczącego odpowiednich elementów, w procesorze użytkownika końcowego, przy wykorzystaniu dostępnych narzędzi statystycznych szacuje się rozkład prawdopodobieństwa *P(a, b | x, y, i)*, przy czym w odbiorniku użytkownika końcowego wszystkie elementy z jego ciągu danych, które posłużyły do oszacowania rozkładu prawdopodobieństwa *P(a, b | x, y, i)* są usuwane, po czym dalej

– na podstawie rozkładu prawdopodobieństwa *P(a, b | x, y i)* w procesorze użytkownika końcowego, przy wykorzystaniu programowania półokreślonego z zastosowaniem hierarchii NPA oblicza się losowość H wyników *a*, przy czym losowość H wyników a mierzona jest przez entropię i określa nieprzewidywalność, będących w posiadaniu odbiornika użytkownika końcowego ciągu liczb, stanowiąc jednocześnie jej certyfikat, przy czym

– w odbiorniku użytkownika końcowego zatrzymuje się liczbę *a* z jego ciągu danych *x, i, a* albo przeprowadza się ekstrakcję losowości w oparciu o dane wejściowe H oraz docelową entropię, po czym

– przekształca się ciąg liczb losowych w krótszy, którego średnia entropia jest większa lub równa H, przy czym długość końcowego ciągu liczb zależy od stosunku wartości danych wejściowych H i docelowej entropii.

Wynalazek został ujęty na rysunku w ujęciu schematycznym, na którym poszczególne figury prezentują:

– fig. 1: system generowania symetrycznego klucza kryptograficznego z wyszczególnionymi elementami systemu,

– fig. 2: sposób generowania symetrycznego klucza kryptograficznego, na której strzałkami przerywanymi oznaczono kierunek standardowej komunikacji, zaś strzałkami ciągłymi kierunek przesyłania stanów kwantowych,

– fig. 3: system generowania liczb losowych z poszczególnymi elementami systemu,

– fig. 4: sposób generowania liczb losowych, gdzie kierunek standardowej komunikacji oznaczono strzałkami przerywanymi, zaś kierunek przesyłania stanów kwantowych strzałkami ciągłymi,

– fig. 5: schemat źródła splątania,

– fig. 6: schemat urządzenia pomiarowego zespołu pośredniczącego IT,

– fig. 7: schemat odbiornika użytkownika końcowego UT w korelacji do centralnego nadajnika jako elementu zespołu centralnego CT,

– fig. 8: schemat przyrządu pomiarowego odbiornika użytkownika końcowego UT,

– fig. 9 i fig. 10: efektywność detekcji odbiornika użytkownika końcowego UT,

– fig. 11: widzialność odbiornika użytkownika końcowego UT.

Jak ujęto na fig. 1, system generowania symetrycznego klucza kryptograficznego tworzony jest przez zespół centralny CT, dwa zespoły pośredniczące: IT-A oraz IT-B, a także użytkownika końcowego UT-A oraz użytkownika końcowego UT-B. Zespół centralny CT oraz zespoły pośredniczące IT-A oraz IT-B tworzą razem laboratorium centralne CL. Zespół centralny CT zawiera wyposażony w procesor główny 1 nadajnik centralny 2 oraz źródło splątania 3. Każdy z zespołów pośredniczących: IT-A oraz IT-B zawiera przekaźnik sygnałów 4, urządzenie pomiarowe 5 oraz koprocesor 6, zaś każdy użytkownik końcowy UT-A oraz użytkownik końcowy UT-B posiada przyrządy pomiarowe 9 oraz procesory 8.

W zaprezentowanym na fig. 2 sposobie generowania symetrycznego klucza kryptograficznego źródło splątania 3 generuje stany kwantowe, które zawierają podsystemy, splątane w polaryzacji. Źródło splątania 3 połączone jest z przekaźnikami sygnałów 4. Generuje ono będącą w stanie splątanym parę fotonów, którą wysyła do obu przekaźników sygnałów 4. Otrzymane ze źródła splątania 3 stany kwantowe każdy przekaźnik sygnałów 4 przesyła do posiadającego funkcjonalność mierzenia stanów kwantowych odpowiedniego urządzenia pomiarowego 5. Skomunikowane z procesorem głównym 1 koprocesory 6 odpowiedzialne są za sterowanie odpowiednimi przekaźnikami sygnałów 4 oraz odpowiednimi urządzeniami pomiarowymi 5. Powiązane z procesorem głównym 1 oba procesory 8 odpowiadają za komunikację z należącymi do innych użytkowników końcowych odbiornikami 7. Opisana w niniejszym przykładzie wykonania komunikacja odbywa się bezprzewodowo. Jak zaznaczono na figurze, każdy przekaźnik sygnałów 4 łączy się z odpowiednim odbiornikiem 7 i w odpowiednim procesorze 8 generuje zapisane w formie cyfrowej ciągi danych, po czym w procesorach 8 wybiera się losową liczbę naturalną *x*, odpowiednio *y*, oraz liczbę binarną *i*, odpowiednio *j*, po czym liczby te wysyłane są do odpowiednich koprocesorów 6. W urządzeniach pomiarowych 5, które otrzymały z odpowiednich przekaźników sygnałów 4 stany kwantowe wykonuje się pomiar *x*, odpowiednio pomiar *y*, a otrzymane wyniki pomiaru oznacza się jako a, odpowiednio b, po czym odsyła się je poprzez odpowiednie koprocesory 6 do odpowiednich procesorów 8. W odbiornikach 7 generuje się ciągi liczb o długości N, a z nich tworzy się klucz kryptograficzny, poprzez wykonanie następujących czynności: w każdym z procesorów 8 z elementów ciągu liczb wybiera się losowo liczbę określającą dokładność oszacowania bezpieczeństwa klucza K, natomiast, dla wszystkich pozostałych elementów w ciągach liczb procesory 8 przesyłają między sobą wartości *x, i*, odpowiednio *y, j*.

Następnie, w obu procesorach 8, po obliczeniu losowości wyników *a*, odpowiednio wyników *b*, korekcji błędów i amplifikacji prywatności generuje się wynik będący symetrycznym kluczem współdzielonym przed odbiorniki 7.

Na fig. 3 ujęto system generowania liczb losowych. Widać zespół centralny CT, dwa zespoły pośredniczące: IT-A oraz IT-B, a także użytkownika końcowego UT-A. Zespół pośredniczący IT-A zawiera przekaźnik sygnałów 4, urządzenie pomiarowe 5 oraz koprocesor 6, zaś zespół pośredniczący IT-B zawiera urządzenie pomiarowe 5 oraz koprocesor 6. Użytkownik końcowy UT-A wyposażony jest natomiast w przyrząd pomiarowy 9 oraz procesor 8.

Jak zaznaczono na fig. 4, użytkownik końcowy UT-A wybiera losową liczbę naturalną *x* oraz liczbę binarną *i*, po czym obie wysyła do zespołu pośredniczącego IT-A. Źródło splątania 3 przygotowuje parę fotonów w stanie splątanym i wysyła je do przekaźników sygnałów 4 w zespołach pośredniczących IT-A oraz IT-B. W zespole pośredniczącym IT-A z przekaźnika sygnałów 4 przesyłany jest stan kwantowy do przyrządu pomiarowego użytkownika końcowego UT-A. który wykonuje pomiar *x*. Wynik pomiaru oznaczany jest jako *a* i odsyłany przez procesor zespołu pośredniczącego IT-A do użytkownika końcowego UT-A. Z kolei koprocesor 6 zespołu pośredniczącego IT-B wybiera losowo liczbę *y*, a jego urządzenie pomiarowe 5 wykonuje pomiar *y*. Wartość *y* oraz wynik pomiaru *b* są następnie zapisywane. Na koniec użytkownik końcowy UT-A oraz zespół pośredniczący IT-B dysponują ciągami liczb o długości N, przy czym użytkownik końcowy UT-A posiada: *x, i, a*, zaś zespół pośredniczący IT-B posiada: *y, b*.

Na fig. 5 ujęto schemat, będącego częścią centralnego nadajnika 2 źródła splątania. Procesor główny 1 steruje laserem o długości fali 405 nm, który wysyła impulsy świetlne przechodzące przez filtr braggowski typu VBG, płytki półfalowe HWP oraz płytki półfalowe QWP, których położenie również kontrolowane jest

przez procesor główny 1. Następnie za pomocą soczewki L promień skupiany jest na lustrze dichroicznym DM, przez które przechodzi do interferometru Sagnaca. W tej części trafia na polaryzacyjne lustro półprzepuszczające PBS, po którym odbija się od luster M, przechodzi przez HWP oraz nieliniowy kryształ ppKTP. Po opuszczeniu interferometru część wiązki bezpośrednio skupiana jest przez L w złączu FC, podłączonym do przekaźnika sygnałów 4B, zaś reszta wiązki trafia znów na DM i przez L skupiana jest na złączu FC, podłączonym do przekaźnika sygnałów 4A.

Na fig. 6 widać schemat urządzenia pomiarowego 5. Wiązka laserowa przychodząca z przekaźnika światłowodem dociera do pełniącego funkcję sprzęgacza złącza FC, który wypuszcza ją ze światłowodu. Soczewka L skupia ją na modulatorze elektrooptycznym EOM, który sterowany jest przez koprocesor 6 i zmienia polaryzację wiązki. Następnie wiązka trafia na polaryzacyjne lustro półprzepuszczalne PBS, gdzie rozdzielana jest na dwie części. Każda za pomocą soczewki L skupiana jest w złączu FC, który wprowadza ją do światłowodu. Światłowody trafiają do umieszczonych w kriostatach detektorów typu TES. Ich sygnał wyjściowy wzmacniany jest przez nadprzewodzące urządzenie interferencyjne qunatum SQUID i wysyłany do koprocesora 6.

Fig. 7 to ujęcie schematu odbiornika 7, który należy do użytkownika końcowego UT oraz stanowiącego element zespołu centralnego CT centralnego nadajnika 2. Uwidoczniono także komunikację jaka występuje pomiędzy nimi. Klasyczna komunikacja cyfrowa oznaczona jest przerywanymi liniami, zaś komunikacja kwantowa, czyli splątane stany kwantowe zakodowane w polaryzacji fotonów oznaczona jest liniami ciągłymi. Na figurze widać także przyrząd pomiarowy 9 oraz procesor 8.

Fig. 8 to prezentacja schematu przyrządu pomiarowego 9. Wiązka laserowa przychodząca z przekaźnika 4 światłowodem dociera do złącza FC,

który wypuszcza ją ze światłowodu. Soczewka L skupia ją na modulatorze elektrooptycznym EOM, który sterowany jest przez procesor 8 i zmienia polaryzację wiązki. Następnie wiązka trafia na polaryzacyjne lustro półprzepuszczalne PBS, gdzie rozdzielana jest na dwie części. Każda za pomocą soczewki L skupiana jest w złączu FC, który wprowadza ją do światłowodu fotodiód lawinowych APD. Wyniki pomiarów przesyłane są do procesora 8.

Fig. 9 ujmuje efektywność detekcji odbiornika użytkownika końcowego UT jako funkcję efektywności detektorów urządzeń pomiarowych zespołów pośredniczących IT-A oraz IT-B, dla różnych wartości efektywności ich detektorów η.

Figura 10, ujawnia także efektywność detekcji odbiornika użytkownika końcowego UT, przy różnych wartościach efektywności detektorów η zespołu pośredniczącego IT oraz jego widzialności v.

Na fig. 11 ujęto widzialność oraz efektywność detekcji odbiornika użytkownika końcowego UT, przy różnych wartościach efektywności detektorów η zespołu pośredniczącego IT oraz stałej widzialności v. Ujęto efektywność detekcji odbiornika użytkownika końcowego UT, wymaganą dla niezerowej losowości, dla różnych wartości efektywności detekcji zespołów pośredniczących IT urządzeń pomiarowych 5, przy widzialności tych urządzeń na poziomie 99,3%.

Wymagania sprzętowe wobec centralnego nadajnika są względnie wysokie, tj. porównywalne lub nieznacznie niższe, niż te stawiane obecnie kryptografii niezależnej od urządzeń. Natomiast wymagania sprzętowe względem odbiorników są dużo mniejsze tj. porównywalne lub nieznacznie niższe niż te stawiane obecnie standardowej kryptografii kwantowej.

W efekcie koszt urządzenia dla użytkownika końcowego jest niższy niż obecnie, przy jednoczesnym zwiększeniu zasięgu z setek metrów do około 100 km.

Wynalazek dotyczy systemu kryptograficznego opartego o zespół centralny, zespoły pośredniczące oraz użytkowników końcowych.

Zespół centralny oraz zespół pośredniczący to centralne laboratorium, które generuje stany kwantowe, zawierające podsystemy, splątane w dowolnym stopniu swobody, a także posiada funkcjonalność mierzenia stanów kwantowych.

Komunikacja w centralnym laboratorium oraz pomiędzy nim a użytkownikami końcowymi może odbywać się za pośrednictwem komunikacji bezprzewodowej lub przewodowej, np. światłowodów.

Urządzenia pomiarowe centralnego laboratorium posiadają wysoko efektywne detektory nadprzewodzące, podczas gdy należące do użytkowników końcowych przyrządy pomiarowe odbiorników mają dostęp jedynie do fotodiod lawinowych.

Ze względu na różnice w kosztach urządzeń pomiarowych wykorzystujących te detektory, gdzie fotodiody lawinowe są prostymi i tanimi urządzeniami, podczas gdy detektory nadprzewodzące wymagają utrzymywania w temperaturze bliskiej zera bezwzględnego, co znacznie zwiększa ich koszty utrzymania, proponowany w wynalazku system jest idealnym rozwiązaniem dla państwa lub regionu, które są w stanie przeznaczyć znaczne fundusze na zapewnienie swoim mieszkańcom bezpiecznej komunikacji, przy jednoczesnym braku potrzeby zakupu przez nich drogich urządzeń.

Rolę procesora głównego w centralnym nadajniku pełni serwer obliczeniowy, który połączony jest z odbiornikami użytkowników końcowych, a także z koprocesorami oraz przekaźnikami sygnałów zespołów pośredniczących.

Źródło splątania oraz urządzenia pomiarowe zespołów pośredniczących oparte są o układ eksperymentalny opublikowany i znany w stanie techniki, źródło: M. Giustina, et. al. Phys. Rev. Lett. 115, 250401 2015.

Źródło splątania odpowiedzialne jest za generację stanów kwantowych. Połączone jest ono z przekaźnikami sygnałów, do których wysyłane są zakodowane w fotonach stany kwantowe.

W przedstawionych w przykładach wykonania procesor główny wysyła sygnały do lasera z częstotliwością 1MHz, który produkuje impuls świetlny o długości fali 405nm i czasie trwania 12ns. Impuls z lasera przechodzi przez elementy optyczne, mające na celu oczyszczenie wiązki z fotonów o niepożądanych właściwościach a także ustawienie stanu kwantowego który maksymalizuje łamanie nierówności CHSH przez urządzenia pomiarowe zespołów pośredniczących.

Ustawienie stanu kwantowego odbywa się poprzez przesuwanie elementów HWP i QWP, przez które przechodzi wiązka pompująca. Optymalny stan kwantowy zależy od efektywności detektorów urządzeń pomiarowych.

Poniżej przedstawiono obliczenia optymalnego stanu kwantowego. W celu lepszego zobrazowania tych obliczeń, urządzenia pomiarowe dwóch zespołów pośredniczących zostały określone jako urządzenie pomiarowe A i urządzenie pomiarowe B.

Optymalny stan kwantowy może zatem zostać obliczony w następujący sposób:

definiuje się operator $\beta\eta=\eta^2\ \beta+\eta(1-\eta)\ A_0+B_0$, gdzie η to efektywność detektorów urządzeń pomiarowych, $\beta=A_0\ B_0+A_0\ B_1+A_1\ B_0-A_1\ B_1$, natomiast, dla $x,y=0,1\ A_x=\cos\theta_x\ X+\sin\theta_x\ Z$, $B_y=\cos\vartheta_y\ X+\sin\vartheta_y\ Z$, gdzie X i Z to macierze Pauliego; następnie przeprowadza się optymalizację numeryczną maksymalnej wartości własnej tego operatora po parametrach θ_x i ϑ_y. Wartości

tych parametrów jednoznacznie definiują bazy pomiarowe wykorzystywane przez urządzenia pomiarowe A i B. Po czym, za pomocą standardowych metod algebry liniowej znajdywany jest wektor własny operatora $\beta\eta$ odpowiadający największej wartości własnej. I właśnie ten wektor definiuje optymalny stan kwantowy. Następnie, wiązka laserowa pompuje nieliniowy kryształ ppKTP umieszczony w interferometrze Sagnaca. Po wyjściu z interferometru, dwie wiązki splątanych w polaryzacji fotonów wysyłane są od przekaźników sygnałów.

Przekaźniki sygnałów połączone są z procesorem głównym oraz z jednym z koprocesorów. Dodatkowo, przekaźniki sygnałów, oprócz wejścia, którym może być światłowód wejściowy, dostarczający fotony ze źródła splątania, posiadają wiele wyjść np. światłowodowych. Jeden z nich prowadzi do urządzenia pomiarowego, a pozostałe do odbiorników. Rolą przekaźników sygnałów jest, zgodne z poleceniami przesyłanymi przez odbiorniki lub procesor główny kierowanie sygnału ze źródła splątania do urządzenia pomiarowego lub odbiornika. W konkretnym zespole pośredniczącym przekaźnik sygnałów połączony jest z koprocesorem, połączonym także z urządzeniem pomiarowym.

Przekaźnik sygnałów zbudowany jest w następujący sposób: światło ze światłowodu przychodzącego ze źródła splątania wysyłane jest na lustro, którego kąt nachylenia regulowany jest przez piezoelektryczny serwomotor, sterowany przez koprocesor połączony z przekaźnikiem. Zależnie od ustawienia piezoelektrycznego serwomotoru światło skupiane jest w światłowód do urządzenia pomiarowego z którym przekaźnik jest połączony lub prowadzący do jednego z odbiorników.

Jak wspomniano powyżej, pojedynczy koprocesor połączone jest z procesorem głównym, jednym z przekaźników sygnałów oraz jednym z urządzeń pomiarowych. Koprocesory odpowiedzialne są za sterowanie przekaźnikami

sygnałów i urządzeniami pomiarowymi oraz komunikację z odbiornikiem, a także z procesorem głównym.

Rolę koprocesora pełni układ FPGA, który wyposażony jest dodatkowo w generator liczb losowych, wykorzystywany do wyboru pomiaru w przypadku, kiedy system działa w trybie generacji liczb losowych.

Urządzenia pomiarowe są identycznymi elementami połączonymi z odpowiednimi koprocesorami oraz z przekaźnikami sygnałów. Urządzenie pomiarowe dokonuje wyboru bazy pomiarowej na podstawie następującej metody:

definiuje się operator $\beta\eta=\eta^2\ \beta+\eta(1-\eta)A_0+B_0$, gdzie η to efektywność detektorów urządzeń pomiarowych A i B, $\beta=A_0\ B_0+A_0\ B_1+A_1\ B_0-A_1\ B_1$, natomiast, dla $x,y=0,1\ A_x=\cos\theta_x\ X+\sin\theta_x\ Z$, $B_y=\cos\vartheta_y\ X+\sin\vartheta_y\ Z$, gdzie X i Z to macierze Pauliego; następnie, po parametrach θ_x oraz ϑ_y przeprowadza się optymalizację numeryczną maksymalnej wartości własnej tego operatora. Wartości tych parametrów jednoznacznie definiują bazy pomiarowe wykorzystywane przez urządzenia pomiarowe. Po czym, za pomocą standardowych metod algebry liniowej znajdywany jest wektor własny operatora $\beta\eta$ odpowiadający największej wartości własnej. Metoda ta podaje kąt θ_x oraz ϑ_y, o jaki należy obrócić polaryzację wiązki dla każdej wartości x oraz y. Obrót ten wykonywany jest poprzez układ EOM, czyli wspomniany powyżej modulator elektrooptyczny. Następnie wiązka pada na polaryzujący rozdzielacz wiązki, który kieruje sygnał do jednego z dwóch detektorów nadprzewodzących TES transition-edge sensor utrzymywanych w temperaturze 100mK. Ich sygnał wyjściowy wzmacniany jest przez nadprzewodzące urządzenie interferencyjne qunatum SQUID superconducting qunatum interference device i wysyłany do jednego z koprocesorów, gdzie zapisywany jest jako wynik a lub b.

Każdy z odbiorników składa się z dwóch podstawowych elementów, tj. procesora oraz przyrządu pomiarowego.

Procesor odbiornika połączony jest z centralnym nadajnikiem oraz z przyrządem pomiarowym i odpowiada za sterowanie przyrządem pomiarowym, komunikację z centralnym nadajnikiem oraz za zbieranie i przetwarzanie danych wyjściowych.

Wybór bazy dokonywany jest przez obrót polaryzacji wiązki o pewien kąt. Kąty obrotu przyrządu pomiarowego odbiornika użytkownika są takie same jak kąty obrotu urządzenia pomiarowego zespołu pośredniczącego. Kąty obrotu odbiornik otrzymuje z centralnego laboratorium na początku pracy. Obrót wykonywany jest poprzez układ EOM. Następnie wiązka pada na polaryzujący rozdzielacz wiązki polarizing beam splitter, który kieruje sygnał do jednego z dwóch detektorów standardowych fotodiod lawinowych, które z kolei dokonują pomiaru, a wynik wysyłają do procesora odbiornika użytkownika.

Centralny nadajnik jest w stanie obsługiwać wiele odbiorników. Kiedy użytkownik będący właścicielem jednego z nich zgłasza zapotrzebowanie na liczby losowe lub para użytkowników na klucz kryptograficzny, zostają oni umieszczeni w kolejce, a zapotrzebowanie zostanie zrealizowane, kiedy przyjdzie ich kolej.

Do generacji symetrycznego klucza oraz liczb losowych metody używane przez procesor odbiornika użytkownika to: programowanie pół-określone używające hierarchii NPA do oszacowania entropii, protokół CASCADE do korekcji błędów, oraz funkcja HMAC opisana w [FIPS PUB 198-1] do amplifikacji prywatności.

Funkcja HMAC wymaga dobrania funkcji haszującej jako jej wewnętrznej procedury. Do tego celu użyta jest funkcja SHA-256 opisana w [FIPS PUB 180-4]. Wynikiem metody jest bezpieczny, symetryczny klucz współdzielony przez

procesory odbiorników a w przypadku generowania liczb losowych wygenerowanie oraz certyfikacja liczb losowych.

Głównym parametrem mierzącym skuteczność jego działania jest entropia wyników otrzymanych przez użytkowników odbiorników. Jakakolwiek niezerowa wartość entropii umożliwi jej późniejszą ekstrakcję do dowolnej, zadawalającej użytkownika wielkości.

W trybie tworzenia klucza kryptograficznego minimalna wymagana dla bezpieczeństwa entropia zależy też od wartości E – korelacji pomiędzy odbiornikami. Dla E = 1 dowolna niezerowa wartość entropii jest wystarczająca, dla mniejszych wartości jest to wyłącznie warunek konieczny.

Z powyższych powodów przeprowadzona analiza działania zgłaszanego wynalazku oparta została na znalezieniu parametrów, które umożliwiają otrzymanie przez użytkowników niezerowej wartości H. W analizie założono, że stany kwantowe produkowane przez źródło splątania są stanami dwóch kubitów, a każdy z zespołów pośredniczących oraz odbiorników użytkowników ma do wyboru dwie możliwe bazy pomiarowe. Inaczej rzecz ujmując: x i y mogą przyjąć tylko dwie wartości.

Umożliwienie użytkownikom i zespołom pośredniczącym wyboru większej ilości baz jest konieczne do efektywnej generacji klucza kwantowego lub liczb losowych, ale ponieważ może to wyłącznie zwiększyć szacowaną wartość H, na tym etapie analizy nie jest to konieczne.

Wykonane przez Zgłaszającego niniejszy wynalazek analityczne obliczenia wykazały, że jeśli krytyczna efektywność detektorów centralnego laboratorium jest większa niż 67%, a stan kwantowy produkowany przez źródło splątania jest optymalnym stanem dla tej efektywności, to dla dowolnej efektywności detektorów użytkowników są one w stanie otrzymać wyniki o

niezerowej entropii. Jakościowe wyniki, otrzymane za pomocą programowania pół-określonego przedstawione są na fig. 9.

W powyższych obliczeniach przyjęte było założenie, że stan produkowany przez źródło splątania jest idealny dla rzeczywistej efektywności detektorów urządzeń pomiarowych. W praktyce nie jest to możliwe, choć przy obecnym stanie techniki osiągane są wartości bardzo zbliżone do ideału. Miarą tego jak blisko stan kwantowy jest zbliżony do optymalnego jest widzialność. Wartość 100% oznacza, że stan jest doskonały.

Na fig.10 przedstawiono wykres entropii odbiorników jako funkcji efektywności ich detektorów dla różnych wartości efektywności urządzeń pomiarowych oraz widzialności odbiorników, przy czym widzialność urządzeń pomiarowych dla wszystkich przypadków wynosi 97,5%.

Wyniki te pokazują, że nawet przy znaczącym spadku widzialności realne jest otrzymanie niezerowej losowości, pomimo posiadania przez użytkowników niskoefektywnych detektorów.

Wykres na figurze 11 przedstawia zależność pomiędzy wymaganą widzialnością i efektywnością odbiornika, które umożliwiają certyfikację niezerowej entropii, dla różnych wartości efektywności detektorów urządzeń pomiarowych. Ich widzialność we wszystkich przypadkach wynosi 98,4%.

Należy dodać, że wynalazek pozwoli także na nową funkcjonalność centralnego laboratorium, niemożliwą do uzyskania przy obecnie używanej technologii – nadajnika certyfikowanej losowości. Zwykłe nadajniki losowości dają odbiorcom dostęp do liczb losowych o wysokiej entropii, czyli takich, których wartości są trudne do wcześniejszego przewidzenia, jednak, ponieważ wysyłane są publicznym kanałem komunikacyjnym, mogą do nich w łatwy sposób uzyskać dostęp osoby trzecie co powoduje, że nie mogą zostać zastosowane w kryptografii.

Nadajnik certyfikowanej losowości zapewni odbiorcy, oprócz liczb o wysokiej entropi, gwarancję, że nikt inny, nawet sam nadajnik nie ma do nich dostępu.

Wynalazek będzie miał swoje zastosowanie do wykonywania czynności kryptograficznych w celu zapewnienia bezpieczeństwa komunikacji w infrastrukturze publicznej.

Marcin Barycki

rzecznik patentowy / pełnomocnik