Certyfikacja prawdziwej losowości za pomocą arbitralnie nieefektywnych detektorów (CGRID)

Podczas logowania się na stronach internetowych każdy z nas spotkał się z irytującymi całkowicie zautomatyzowanymi publicznymi testami Turinga do rozróżniania komputerów i ludzi (CAPTCHAs). Testy te są dość prymitywnymi schematami kryptograficznymi, których celem jest określenie, czy użytkownik jest człowiekiem, czy botem. Załóżmy, że sztucznie inteligentny przeciwnik, który chce oszukać użytkownika, może z góry przewidzieć, jakie CAPTCHA się pojawią. W takim przypadku systemy te staną się całkowicie bezużyteczne i niezabezpieczone. Innymi słowy, skuteczność tych testów, podobnie jak naszych pinów bankowych i jednorazowych identyfikatorów (OTP), opiera się na bezpiecznych liczbach losowych. Prawdziwie nieprzewidywalne liczby losowe są niezbędne w każdym kryptosystemie, a tym samym dla prywatności i bezpiecznej komunikacji, które stanowią fundamenty współczesnej cywilizacji demokratycznej.

Jednak w świecie klasycznym nie istnieje coś takiego jak prawdziwa przypadkowość. Wszystkie klasyczne procesy fizyczne są zasadniczo deterministyczne i tylko z powodu braku wiedzy wydają się przypadkowe. W związku z tym wszystkie klasyczne generatory liczb losowych (CRNG) są podatne na ataki typu back-door. Złośliwy producent lub przeciwnik mający dostęp do CRNG może łatwo odgadnąć liczby losowe i naruszyć bezpieczeństwo kryptosystemów, które na nich bazują. Dlatego też generowanie liczb losowych musi być oparte na certyfikowanych, nieprzewidywalnych procesach fizycznych, aby zapewnić trwałą prywatność i bezpieczną komunikację. Dzięki temu liczby losowe pozostaną bezpieczne nawet dla wszechmocnego przeciwnika, którego ograniczają jedynie prawa fizyki. Mechanika kwantowa jest teorią z natury losową, a kwantowe procesy fizyczne stanowią doskonałą podstawę dla generatorów liczb losowych (QRNG). Jednak naiwne QRNG wymagają od użytkowników zaufania do producenta urządzenia, co nie jest najlepszym pomysłem.

Jedynym rozwiązaniem jest kryptografia kwantowa niezależna od urządzeń (DI), w której bezpieczeństwo kryptosystemu nie zależy od wewnętrznego działania urządzeń. W szczególności bezpieczeństwo schematów DIQRNG polega wyłącznie na nieklasyczności obserwowanych statystyk. Jednak w schematach DIQRNG, które opierają się na statystycznych testach nieklasyczności, występują luki. Najważniejszą z nich jest luka efektywności detekcji (DEL), która polega na tym, że sprytny przeciwnik może wykorzystać straty eksperymentalne do sfałszowania nieklasyczności, przez co schematy DIQRNG nie są bezpieczne. Aby udaremnić takie ataki, detektory kwantowe w DIQRNG muszą mieć minimalną sprawność progową, zwaną krytyczną sprawnością detekcji (CDE). Niestety, CDE są zazwyczaj bardzo wysokie w porównaniu z możliwościami najnowocześniejszego sprzętu, co sprawia, że praktyczna kryptografia DI jest niewykonalna w bliskiej przyszłości.

CGRID to przełomowy projekt, który ma zaradzić tej sytuacji i uczynić kryptografię DI możliwą do zastosowania w najbliższej przyszłości. Projekt ten wprowadzi bezprecedensowe, wysokowydajne schematy DIQRNG, charakteryzujące się zerowymi wymaganiami CDE i wysoką odpornością na niedoskonałości eksperymentalne, co zasadniczo pozwoli nam na uzyskiwanie bezwarunkowo bezpiecznych liczb prawdziwie losowych przy użyciu bardzo nieefektywnych detektorów. W szczególności, przedstawimy rewolucyjne ramy dla 1) kryptografii DI z wieloma użytkownikami, którzy mogą wspólnie kontrolować przepływ informacji kwantowej w sieci oraz 2) kryptografii semi-DI opartej na założeniach, które mogą być operacyjnie sprawdzone. Do analizy bezpieczeństwa i skuteczności tych schematów wykorzystamy najnowocześniejsze metody analityczne i numeryczne. Narzędzia te zostaną udostępnione publicznie, z korzyścią dla społeczności naukowej i potomnych. Aby zademonstrować możliwość zastosowania tych nowych schematów w świecie rzeczywistym, we współpracy z Uniwersytetem w Concepción w Chile przeprowadzimy eksperymentalną demonstrację ich dowodów słuszności na fotonicznych systemach kwantowych.

W dzisiejszych czasach, gdy szybki postęp technologiczny zagraża prywatności jednostki, będącej filarem współczesnej cywilizacji demokratycznej, Natura dostarcza rozwiązanie w postaci kryptografii kwantowej. CGRID sprawi, że w niedalekiej przyszłości kryptografia kwantowa stanie się powszechnie stosowaną, niezawodną technologią, która zagwarantuje bezpieczną komunikację i prywatność na wieczność, a przynajmniej do czasu, gdy prawa fizyki nie przestaną obowiązywać.