Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 51-63 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

THE MODEL NEW QUANTUM RANDOM NUMBER GENERATOR WITH THE CORRESPONDING VERIFICATION METHOD.

Tamari Kuchukhidze, Georgian Technical University, Scientific Cyber Security Association
Tbilisi, Georgia

ABSTRACT: Random number generators are widely used in various fields including encryption, statistical analysis and numerical simulations. They are also a fundamental resource in science and engineering.
There are algorithmically generated numbers that look like random numbers but are not truly random, called pseudo random number generators. In cases where true randomness is necessary, we use true random number generators, where unpredictable random events are used as a random source.
Quantum Random Number Generators (QRNGs) generate real random numbers based on the inherent randomness of quantum measurements. Our goal is to generate fast random numbers at a lower cost. At the same time, a high level of randomness is essential.
It is essential to trust cryptographic random number generators to generate only true random numbers. This is why certification methods are needed which will check both the operation of the device and the quality of the random bits generated.
We present the improved novel quantum random number generator, which is based the on time of arrival QRNG. It is rather efficient, as it uses the simple version of the detectors with rather few requirements. The novel QRNG produces more than one random bit per each photon detection.
Self-testing as well as device independent quantum random number generation methods are analyzed. The advantages and disadvantages of both methods are identified. The model of a novel semi self-testing certification method for quantum random number generators (QRNG) is offered in the paper. This method combines different types of certification approaches and is rather secure and efficient. The paper analyzes its security and efficiency.

KEYWORDS: *quantum, random number generator, quantum random number generator, novel quantum random number generator, certification.*

რეზიუმე: შემთხვევითი რიცხვის გენერატორები ფართოდ გამოიყენება სხვადასხვა სფეროში, მათ შორის დაშიფვრა, სტატისტიკური ანალიზი და რიცხვითი სიმულაციები. ისინი ასევე ფუნდამენტური რესურსია მეცნიერებასა და ინჟინერიაში.
არსებობს ალგორითმულად გამომუშავებული ციფრები, რომლებიც შემთხვევითი განაწილების მსგავსია, მაგრამ სინამდვილეში შემთხვევითი არ არის, რომლებსაც ფსევდო შემთხვევითი რიცხვის გენერატორებს უწოდებენ. იმ შემთხვევებში, როცა ჭეშმარიტი შემთხვევითობა აუცილებელია, ჩვენ ვიყენებთ ნამდვილ შემთხვევითი რიცხვის გენერატორებს. ამ შემთხვევაში, არაპროგნოზირებადი შემთხვევითი მოვლენებია, როგორც შემთხვევითი წყარო.
კვანტური შემთხვევითი რიცხვის გენერატორებმა (QRNG) გამოაქვთ ნამდვილი შემთხვევითი რიცხვები კვანტური გაზომვების თანდაყოლილი შემთხვევითობის

საფუძველზე. ჩვენი მიზანია სწრაფი შემთხვევითი რიცხვების გენერირება უფრო დაბალ ფასად. ამავე დროს, აუცილებელია შემთხვევითობის მაღალი დონე.
საჭიროა ვენდოთ კრიპტოგრაფიული შემთხვევითი რიცხვის გენერატორებს, რომ ისინი წარმოქმნიან მხოლოდ ჭეშმარიტი შემთხვევითი რიცხვებს. ამიტომ გვჭირდება სერთიფიცირების მეთოდები, რომლებიც შეამოწმებს როგორც მოწყობილობის მუშაობას, ასევე წარმოქმნილი შემთხვევითი ბიტების ხარისხს.
ჩვენ წარმოგიდგენთ გაუმჯობესებულ ახალ კვანტურ შემთხვევითი რიცხვების გენერატორს, რომელიც ემყარება QRNG ჩამოსვლის დროს. ეს საკმაოდ ეფექტურია, რადგან იყენებს დეტექტორების მარტივ ვერსიას, საკმაოდ მცირე მოთხოვნებით. ახალ QRNG -ს შეუძლია ერთზე მეტ შემთხვევით ბიტის გამოვლენა თითოეულ ფოტონის აღმოჩენისას.
გავაანალიზებთ როგორც თვითტესტირებას, აგრეთვე მოწყობილობაზე დამოუკიდებელი კვანტური შემთხვევითი რიცხვის წარმოქმნის მეთოდებს. განვიხილავთ ორივე მეთოდის დადებით და უარყოფითი მხარეებს. ნაშრომში მოცემულია ახალი ნახევრად თვითტესტირების სერთიფიცირების მეთოდის მოდელი კვანტური შემთხვევითი რიცხვის გენერატორებისთვის (QRNG). ეს მეთოდი აერთიანებს სხვადასხვა ტიპის სერთიფიკაციის მიდგომებს, საკმაოდ უსაფრთხო და ეფექტურია. ნაშრომი აანალიზებს მის უსაფრთხოებასა და ეფექტურობას.

საკვანძო სიტყვები: *კვანტური, შემთხვევითი რიცხვების გენერატორები, კვანტური შემთხვევითი რიცხვების გენერატორები, ახალიკვანტური შემთხვევითი რიცხვების გენერატორები, სერტიფიკაცია.*

1. შესავალი

შემთხვევითი რიცხვები ფართოდ გამოიყენება სხვადასხვა სფეროში, მაგალითად, სიმულაცია, კრიპტოგრაფია, ფუნდამენტური მეცნიერება [1,2]. ალგორითმულად გამომუშავებული რიცხვები ჰგავს შემთხვევით რიცხვებს, მაგრამ ისინი ნამდვილად არ არიან შემთხვევითი; მათ ფსევდო შემთხვევით რიცხვებს უწოდებენ. ეს რიცხვები წარმოიქმნება კომპიუტერის გამოყენებით, დეტერმინესიული ალგორითმების საშუალებით, რომლებსაც ფსევდო შემთხვევითი რიცხვის გენერატორებს უწოდებენ [3-5]. რადგან, ჩვენ არ შეგვიძლია გამოვიყენოთ ფსევდო შემთხვევითი გენერატორები ისეთ სიტუაციებში, როდესაც ჭეშმარიტი შემთხვევითი შემთხვევაა საჭირო, ჩვენ ვიყენებთ ნამდვილი შემთხვევითი რიცხვის გენერატორებს. ამ შემთხვევაში, ჩვენ ვიყენებთ არაპროგნოზირებად შემთხვევით მოვლენებს, როგორც შემთხვევით წყაროს.

ზოგიერთ პროგრამაში, მაგალითად კვანტური კრიპტოგრაფია, ყველა ჭეშმარიტი შემთხვევითი რიცხვის გენერატორი არ არის კრიპტოგრაფიულად დაცული. ჩვენ შეგვიძლია გამოვყოთ TRNG ტიპის QRNG, რომელიც კვანტურ პროცესებში იყენებს თანდაყოლილ შემთხვევითობას, როგორც შემთხვევით წყაროს. არსებული QRNG– ების უმეტესობა ემყარება

კვანტურ ოპტიკას. სინათლის კვანტური მდგომარეობის ბევრ პარამეტრს აქვს თანდაყოლილი შემთხვევითობა, რის შედეგად მრავალი ვარიანტი შეგვიძლია განვახორციელოთ. ლაზერების, დიოდების ან ფოტონის სხვადასხვა წყაროდან მიღებული სინათლე უფრო ხელმისაწვდომია, ვიდრე რადიოაქტიური მასალა. სინათლის ნაწილაკები გამოიყენება კვანტური შემთხვევითობის წყაროდ და ხელმისაწვდომია მრავალი დეტექტორისთვის. შედეგად, ოპტიკური კვანტური შემთხვევითი გენერატორები უფრო სწრაფი და ეფექტურია [6].

საჭიროა ვენდოთ კრიპტოგრაფიული შემთხვევითი რიცხვის გენერატორებს, რომ ისინი წარმოქმნიან მხოლოდ ჭეშმარიტი შემთხვევითი რიცხვებს. მომხმარებლები სრულად უნდა ენდობოდნენ ფსევდო შემთხვევითი რიცხვის გენერატორების ან მოწყობილობის ალგორითმებს, რომელიც ახორციელებს ჭეშმარიტად შემთხვევითი რიცხვების გენერირების მეთოდს. შეგვიძლია ჩვენ თავიდან შევქმნათ შემთხვევითი რიცხვების გენერატორი, მაგრამ ეს არასასურველია. უკვე არსებობს მრავალი საიმედო ალგორითმი და მოწყობილობა, რომლებმაც გაუძლეს წლების განმავლობაში კრიპტანალიზისა და თავდასხმის მცდელობებს.

ეს ნიშნავს, რომ მომხმარებელი უნდა ენდოს მოწყობილობას ან ალგორითმს. პრობლემა, რომელიც თეორიულად ან მარტივად გამოიყურება, შეიძლება ადვილად არ გამოსწორდეს. ბოლოდროინდელმა მოვლენებმა აჩვენა, რომ RNGs მაცდური სამიზნეა ფარული შეტევებისთვის [7-9].

ჩვენ გვაქვს მაგალითები მოწყობილობის დონის თავდასხმის შემთხვევაში, თუ როგორ შეძლო არაკეთილსინდისიერმა მწარმოებელმა ან რომელიმე თავდამსხმელმა შეცდომა გამოიწვიოს მოწყობილობაში შესვლისას. ასეთ ტექნიკურად განვითარებულ შეტევაში თავდამსხმელს შეეძლო დაუშვა შეცდომები, რომელთა ამოცნობაც რთულია რეალურ სამყაროში RNG– ებში.

ფიზიკური შემთხვევითი რიცხვის გენერატორებისთვის გვაქვს ისეთი პრობლემები, როგორიცაა შესაძლო სპონტანური შეწყვეტა. თუ მოწყობილობის კომპონენტი შეწყვეტს მუშაობას ან დეგრადირდება, გამომავალი ბიტების ხარისხი შეიძლება შეიცვალოს. თუ მოწყობილობა ქმნის მნიშვნელობებს, მოწყობილობის ფარული ხარვეზების გამოვლენა განსაკუთრებით რთულია. ამ მიზეზით, უსაფრთხოების რეკომენდაციები საჭიროებს ერთგვარ თვით ტესტირებას ნამდვილი კვანტური რიცხვის გენერატორებში. ქვესისტემამ უნდა გააკონტროლოს მოწყობილობის მდგომარეობა ნებისმიერ დროს.

ნაშრომის მიზანია სწრაფი შემთხვევითი რიცხვების გენერირება დაბალ ფასად. შემთხვევითობის მაღალი დონე სავალდებულოა. ჩვენ წარმოგიდგენთ გაუმჯობესებულ ახალ კვანტურ შემთხვევითი რიცხვების გენერატორს, რომელიც ემყარება მოსვლის დროზე დაფუძნებულ. ეს საკმაოდ ეფექტურია, რადგან იყენებს დეტექტორების მარტივ ვერსიას, საკმაოდ მცირე მოთხოვნებით. ახალ QRNG -ს შეუძლია ერთზე მეტ შემთხვევით ბიტის გამოვლენა თითოეულ ფოტონის აღმოჩენისას.

შევისწავლეთ არასანდო მოწყობილობებთან მუშაობის კვანტური გზები. პირველად გაანალიზებულია QRNG- ის თვითტესტირების მეთოდი, შემდეგ კი მოწყობილობაზე დამოუკიდებელი კვანტური შემთხვევითი რიცხვის გენერატორების ანალიზი. განვიხილეთ კვანტური სერტიფიკაციის სხვადასხვა ფორმები. ამ მეთოდების საფუძველზე შემოგთა კვანტური სვაზებთ ერტიფიკაციის ახალი მეთოდს [10].

2. შემთხვევითი რიცხვების გენერატორები

შემთხვევითი რიცხვის გენერატორები ფართოდ გამოიყენება სხვადასხვა სფეროში, მათ შორის დაშიფვრა, სტატისტიკური ანალიზი და რიცხვითი სიმულაციები. არსებობს ალგორითმულად გამომუშავებული ციფრები, რომლებიც შემთხვევითი განაწილების მსგავსია, რომლებსაც ფსევდო შემთხვევითი რიცხვის გენერატორებს უწოდებენ და არის შემთხვევითი რიცხვები, რომლებიც წარმოიქმნება არაპროგნოზირებადი ფიზიკური მოვლენების შედეგად. იმის გამო, რომ ჩვენ არ შეგვიძლია გამოვიყენოთ ფსევდო შემთხვევითი გენერატორები ისეთ სიტუაციებში, სადაც ჭეშმარიტი შემთხვევითი შემთხვევაა საჭირო, ჩვენ ვიყენებთ ნამდვილი შემთხვევითი რიცხვის გენერატორებს. ამ შემთხვევაში, არაპროგნოზირებადი შემთხვევით მოვლენები გამოიყენება როგორც შემთხვევითობის წყაროს.

მეთოდებს, რომლებიც წარმოქმნიან შემთხვევითი რიცხვებს დეტერმინული ალგორითმებიდან, ეწოდება ფსევდორანდომული რიცხვის გენერატორი (PRNG). ბუნებრივია, რომ ალგორითმის მიერ გამომუშავებული თანმიმდევრობა ჭეშმარიტად არ არის შემთხვევითი, ხშირ შემთხვევაში ამ ტიპის შემთხვევითობა საკმარისია. სიჩქარის დიდი უპირატესობის გამო, ხშირად გამოიყენება ასეთი გენერატორი, დეტერმინირებული მეთოდი, რომელიც ბაძავს ნამდვილად შემთხვევითი წყაროს მოსალოდნელ ქცევას [11].

PRNG ეფექტურია, შეუძლია მოკლე დროში შექმნას მრავალი რიცხვი. განსაკუთრებით ისეთ შემთხვევაში, თუ გვინდა ბევრი შემთხვევითი რიცხვი, ან მოგვიანებით აუცილებელია არსებული განაწილების გამეორება. ფსევდო შემთხვევითი რიცხვის გენერატორები პერიოდულია, რაც არ არის სასურველი მახასიათებელი, თუმცა, ხანგრძლივი პერიოდის შემთხვევაში, მას თავიდან ავიცილებთ.

PRNG განკუთვნილია ისეთი პროგრამებისთვის, როგორიცაა სიმულაცია და მოდელირება. PRNG არ არის შესაფერისი განხორციელებებისთვის, სადაც ციფრები უნდა იყოს არაპროგნოზირებადი, როგორიცაა მონაცემთა დაშიფვრა და აზარტული თამაშები. ასეთ შემთხვევებში საჭიროა ჭეშმარიტი შემთხვევითი რიცხვის გენერატორების (TRNG) გამოყენება.

TRNG იყენებს რეალურ არაპროგნოზირებად ან ძალიან რთულად პროგნოზირებად რეალურ პროცესებს, შემთხვვევითი თანმიმდევრობების წარმოქმნის მიზნით. ისინი ეყრდნობიან

არაპროგნოზირებად მნიშვნელობებს, რომლებიც კომპიუტერში, პროგრამაში ან სპეციალურ მოწყობილობებშია დაყენებული და გადაეცემა ოპერაციულ სისტემებს. ჭეშმარიტი შემთხვევითი რიცხვის გენერატორები შედგება ორი კომპონენტისგან: არაპროგნოზირებადი წყარო მაღალი ენტროპიით და ფუნქცია, რომელიც გვაძლევს თანაბარი განაწილების მიახლოებას [12,13].

კლასიკური მოვლენები ვერ ჩავთვლით ჭეშმარიტად შემთხვევითად. საეჭვოა, ფიზიკური პროცესი ნამდვილად შემთხვევითია თუ მისი პროგნოზირება ძალიან რთულია. თუ გვინდა ვიყოთ დარწმუნებული გამომავალი რიცხვების შემთხვევითობაში, უნდაგამოიყენეთ კვანტური შემთხვევითი რიცხვების გენერატორები. ეს არის TRNG– ის განსაკუთრებული შემთხვევა, როდესაც მონაცემები მიიღება კვანტური მოვლენის შედეგად. სხვა ფიზიკური სისტემებისგან განსხვავებით, ნამდვილი შემთხვევითობა კვანტური მექანიკის მნიშვნელოვანი ნაწილია. კვანტური შემთხვევითი რიცხვის გენერატორები გამოირჩევიან ამ ასპექტით, კარგად განსაზღვრული თანდაყოლილი, მემკვიდრეობით მიღებული შემთხვევითი პროცესების გამოყენებით, ბიტების წარმოსაქმნელად.

3. კვანტური შემთხვევითი რიცხვების გენერატორები.

PRNG– ს უმეტესობას არ შეუძლია შექმნას კრიპტოგრაფიულად დაცული შემთხვევითი რიცხვები [14-16]. არსებობს კრიპტოგრაფიაში ფსევდო-შემთხვევითი რიცხვის გენერატორების გამოყენების გზები. ალგორითმული გენერატორები, რომლებიც აკმაყოფილებენ დამატებით კრიტერიუმებს, ეწოდება კრიპტოგრაფიულად უსაფრთხო ფსევდორანდომიული გენერატორების, CSPRNG- ებს.

ფიზიკური შემთხვევითი რიცხვების გენერატორები, ასევე კვანტური შემთხვევითი რიცხვების გენერატორებიც შეიძლება გამოვიყენოთ როგორც საწყისი მნიშვნელობები CSPRNG– ებისთვის [17,18]. მაგრამ სიფრთხილე უნდა მივიღოთ. ზოგიერთი შეტევა უტევს TRNG– ებს და მგრძნობიარეა გარემო პირობებიდან მიღებულ ცვლადების მიმართ. არსებობს QRNG ონლაინ ტესტები, რომლებიც ამოწმებენ აკმაყოფილებს თუ არა BSI AIS 20/31 სტანდარტს. სანამ ეს ასპექტები გაითვალისწინება, მრავალი QRNG გვთავაზობს გასაღებების უშუალო წარმოქმნას გარკვეული ტიპის დამუშავების შემდეგ.

შემუშავებულია მრავალი სტატისტიკური ტესტი RNG შედეგების შემთხვევითობის შესამოწმებლად, მაგრამ RNG ტესტირება არ იძლევა უტყუარ შედეგებს. ამრიგად, ჭეშმარიტი შემთხვევითობის მიღება შესაძლებელია მხოლოდ ისეთი პროცესების საშუალებით, რომლებსაც თანდაყოლილი შემთხვევითობა გააჩნიათ. ასეთი წყაროა კვანტური შემთხვევითი რიცხვის გენერატორი.

4. ოპტიკური კვანტური შემთხვევითი რიცხვების გენერატორები.

ჭეშმარიტი შემთხვევითობა შეიძლება წარმოიშვას ნებისმიერი კვანტური პროცესისგან, რომელიც მდგომარეობების თანმიმდევრულ სუპერპოზიციას არღვევს. დღესდღეობით, ხელმისაწვდომია მაღალი ხარისხის ოპტიკური კომპონენტებია, ამიტომ ყველაზე პრაქტიკული QRNG- ები ხორციელდება ფოტოსისტემებში.

კოჰერენტული მდგომარეობა, რომელსაც კლასიკური სინათლის მრავალი თვისება იზიარებს, შეიძლება დაიწეროს რიცხვითი მდგომარეობის სუპერპოზიციაში

$$|\alpha>=e^{-\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n>$$

სადაც α კომპლექსური რიცხვია, n ფოტონების რაოდენობა. ამპლიტუდა $|\alpha|^2$ შეესაბამება მდგომარეობაში ფოტონების საშუალო რაოდენობას. სუსტი ლაზერის სინათლე ახლოს არის კოჰერენტულ მდგომარეობასთან. შეგვიძლია გამოვიყენოთ ლაზერისგან მიღებული კოჰერენტული მდგომარეობა, ერთი ფოტონის მდგომარეობის მისაღებად, თუ საკმარისად დაბალ ინტენსივობას შევარჩევთ.

ხშირ შემთხვევაში გვაინტერესებს მხოლოდ არაკოლერირებული ფოტონების გამომუშავება. ამ შემთხვევაში, LED–დან მიღებული სინათლე ვალიდურია მანამ, სანამ მანძილი ფოტონების წარმოშობიდან უფრო მეტია, ვიდრე წყაროს კოჰერენტული დრო.

მრავალ ტექნოლოგიას შეუძლია შექმნას და გამოავლინოს ერთი ფოტონი, მაგალითად: ფოტომულტიპლიკაციური მილები (PMT), SPAD, ზეგამტარი ნანოსადენების დეტექტორები. ეს არის პოპულარული დეტექტორების მაგალითები.

ტრადიციულად, ერთ ფოტონის დეტექტორებს აქვთ ფოტონის დათვლის შეზღუდული შესაძლებლობა. შემთხვევითობის მიღება ისეთი კვანტური მდგომარეობებიდანაც შეიძლება, რომლებიც მრავალ ფოტონს შეიცავს. არის გაუმჯობესებული დეტექტორები, მაგრამ ძვირია. აპლიკაციების უმეტესობა ფოტონის გამოვლენის ოროობით მიდგომას იყენებს. ერთი ფოტონის დეტექტორების შემდეგი შეზღუდვაა ფოტონების გამოვლენის შემდეგ აღდგენისთვის საჭირო დრო, რომელსაც ეწოდება მკვდარი დრო.

5. ახალი კვანტური შემთხვევითი რიცხვების გენერატორები.

ჩვენი მიზანია უფრო დაბალ ფასად მოვახდინოთ სწრაფი შემთხვევითი რიცხვების გენერირება. ამავე დროს, აუცილებელია შემთხვევითობის მაღალი დონე. ნებისმიერი კვანტური პროცესის დარღვევა იწვევს ჭეშმარიტ შემთხვევითობას, მაგრამ წარმოქმნის სიხშირე დამოკიდებულია დეტექტორის წარმოებაზე [19].

ჩვენ გთავაზობთ გაუმჯობესებულ კვანტურ შემთხვევითი რიცხვების გენერატორს, რომელიც ემყარება QRNG ჩამოსვლის დროს. საუკეთესო შემთხვევაში, თითოეული გამოვლენილი ფოტონიდან ვიღებთ მხოლოდ ერთ შემთხვევით ბიტს, ეს ალბათობა მცირდება დეტექტორის არაეფექტურობით ან მკვდარი დროით. უმეტეს შემთხვევაში, შემთხვევითი რიცხვის გენერატორების სიხშირე იზომება მეგაბაიტებით, რაც არ არის საკმარისი სწრაფი პროგრამებისთვის, როგორიცაა QKD. თუ მრავალ დეტექტორს გამოვიყენებთ უფრო მეტი შემთხვევითი ბიტების შესაქმნელად, ჩვენ გვექნება მიკერძოება, რომელიც წარმოიქმნება დეტექტორების სხვადასხვა ეფექტურობის შედეგად. ერთი დეტექტორის გამოყენებით და გამოვლენის დროის სამი წარმატებული მოვლენის შედარებით, შეგვიძლია გამოვრიცხოთ ეს მიკერძოება. საკმაოდ მოსახერხებელია დეტექტორების მარტივი ვერსიის გამოყენება, რომელსაც შედარებით მცირე მოთხოვნები გააჩნია. ჩვენ გთავაზობთ გამოვიყენოთ ტექნოლოგია, რომელიც გამოიყენება დასუსტებული პულსის კვანტური შემთხვევითი რიცხვის გენერატორებში.

ჩვენ გთავაზობთ OQRNG– ს, რომელსაც სინათლის სუსტი წყარო გააჩნია და ფოტონის გენერაციის ან არ წარმოქმნის ალბათობა თანაბარია. ისე, რომ ერთი ფოტონის მდგომარეობა უნდა იყოს:

$$\frac{|0>_1+|1>_1}{\sqrt{2}}$$

შეგვიძლია მივანიჭოთ 0 თუკი არ მოხდა აღმოჩენა, ხოლო 1 თუ დაკლიკება მოხდა. არ გვაინტერესებს რამდენი ფოტონი გამოვიყენეთ. სუპერპოზიციის დაწერა შეიძლება შემდეგნაირად:

$$\frac{1}{\sqrt{2}}|0>_1+\sum_{c=1}^{\infty}\alpha_c\,|c>_1$$

სადაც $\sum_{c-1}^{\infty}|\alpha_c|^2=\frac{1}{2}$ ვალიდურია. პირველი დაჭერისას ვიღებთ და არ გვაინნტერესებს ერთმა ფოტონმა გამოიყვია თუ მრავალმა. α ამპლიტუდის კოჰერენტული მდომარეობისთვის, ფოტონის პოვნის ალბათობაა 0 თუ

$$pr(n=0)=e^{-|\alpha|^2}$$

ერთი ამ მეტი ფოტონის პოვნის ალბათობაა

$$pr(n\geq 1)=(1-e^{-|\alpha|^2})$$

ყველაზე მარტივი იდეაა ვიპოვოთ α, რომლისთვისაც pr(n = 0) = pr (n ≥ 1). ამ ფორმულისთვის $\alpha=\sqrt{ln2}$. სასურველ აღმოჩენის ალბათობას გვაძლევს პუასონური წყარო, სადაც ψT = ln2 ≈ 0.693.

პრაქტიკაში, გენერატორი მუშაობს ეფექტურ საშუალო ფოტონთა რიცხვზე $\eta\psi T$ დეტექტორზე, η ეფექტურობით. ფონ ნოიმანის ექსტრაქცია უნდა გამოვიყენოთ, რომ არ გვქონდეს მუშაობის პროცესში მიკერძოება. ფოტონის ორი აღმოჩენისთვის, სადაც მათი რაოდენობა n_1 და n_2 -ია, გამომავალი მნიშვნელობაა 1, თუ $n_1 > 0$ და $n_2 = 0$ და 0 თუ $n_1 = 0$ და $n_2 > 1$. შედეგები, ორი თანმიმდევრული ცარიელი პერიოდით ან ორი დაწკაპებით უგულვებელყოფილია. პუასონური წყაროსთვის, ეს ორივე ბიტის მნიშვნელობა შეიძლება მოხდეს ალბათობით $pr(n > 0)pr(n = 0) = e^{-\eta\psi T}(1 - e^{-\eta\psi T})$. შედეგად მიღებული ბიტევის სიჩქარე ოთხჯერ მაინც ნელია, მაგრამ ყველანაირი მიკერძოებისგან თავისუფალი.

ეფექტურობის გასაუმჯობესებლად გთავაზობთ გენერატორის გამოყენებას, რომელიც ფოტონის გამოვლენის შემდეგ ერთზე მეტ შემთხვევით ბიტს წარმოქმნის. ასეთი ტიპისაა ფოტონის დათვლის კვანტური შემთხვევითი რიცხვების გენერატორები. მიღებული შედეგები დაიყოფა ჯგუფებად, რომლებსაც თანაბარი ალბათობა აქვთ. ამ შემთხვევაში, ჩვენ შეგვიძლია გამოვიყენოთ ერთი დეტექტორი მონაცემების გენერაციისთვის. ჩვენ შეგვიძლია ავიღოთ ფოტონების მოსვლის დრო, როგორც კვანტური შემთხვევითი ცვლადი. წარმატებული ფოტონის დრო შეიძლება დაიყოს დროის ბინებად, შექმნილი მრიცხველის მიერ, რომელიც მუშაობს დეტექტორის პარალელურად. მოცემული აღმოჩენის დროის ინტერვალი გვაძლევს რამდენიმე ბიტს თითო აღმოჩენისთვის. ამ პროცესში მოვლენები ვითარდება დამოუკიდებლად, არის პუასონური პროცესი [20].

შემთხვევითი რიცხვის წარმოქმნის სიხშირის გასაზრდელად გთავაზობთ გაზომვების ჩატარებას მაღალგანზომილებიან კვანტურ სივრცეში, მაგალითად ფოტონის დროით და სივრცული რეჟიმში. ფოტონის მოსვლის დროის გაზომვით, ვიღებთ შემთხვევით ბიტებს დროის ინტერვალის, Δt, ორი მოვლენის აღმოჩენის შედეგად. დროითი რეჟიმის შემთხვევაში ერთი ფოტონის გამოვლენისას შეგვიძლია ერთზე მეტი შემთხვევითი ბიტი მივიღოთ. ფოტონის სივრცული რეჟიმის გამოყენებით, შეგვიძლია მივითოთ შემთხვევითი რიცხვები დეტექტორის მატრიცაში პარალელურად. ამ მეთოდის გამოყენებისას უმჯობესია ყურადღება მიაქციოთ მკვდარ დროს, რადგან ეს გავლენას ახდენს დეტექტორის მრიცხველის სიჩქარეზე [21].

გაუმჯობესებული სიხშირე გვეხმარება არჩევანის გაკეთებაში, თუ რამდენი ბიტი გამოვიყენოთ დათვლილი რაოდენობის ფოტონებიდან და მივიღოთ შემთხვევითობის მაღალი დონე.

6. ახალი ნახევრად თვითტესტირების მეთოდი

ჭეშმარიტი შემთხვევითობა შეუძლებელია მხოლოდ კლასიკური მექანიკის პროცედურებით, ამიტომ ვიყენებთ კრიპტოგრაფიულ პროტოკოლებს. კვანტური შემთხვევითი გენერატორები, მოწყობილობის სანდოობის მიხედვით, შეიძლება დაიყოს რამდენიმე კატეგორიად. პირველია თვით ტესტირებადი QRNG, რომელიც არ არის დამოკიდებული მოწყობილობაზე.

ამ ტიპის QRNG–ის უპირატესობა არის თვითტესტირების შემთხვევითი თვისება. მაგრამ, როგორც წესი, მისი გენერაციის მაჩვენებელი ძალიან დაბალია. მეორე კატეგორია არის მოწყობილობისგან დამოუკიდებელი კვანტური შემთხვევითი რიცხვის გენერატორები. იგი შექმნილია სრულიად საიმედო მოწყობილობებით და შეუძლია მიაღწიოს მაღალი გენერაციის სიჩქარეს, თუ მოწყობილობა სწორად არის მოდელირებული. წინააღმდეგ შემთხვევაში, როდესაც მოწყობილობას მოწინააღმდეგები აკონტროლებენ, შედეგი აღარ იქნება შემთხვევითი.

ამ ორ მიდგომას გააჩნია, როგორც დადებითი, ასევე უარყოფითი მხარეები. რეალურად განხორციელებისას, უფრო მისაღებია ავიღოთ გარკვეული მახასიათებლები და რაღაც შუალედური სერთიფიცირების მეთოდის გამოვიყენოთ. პრაქტიკული, მოწყობილობისგან დამოუკიდებელი კვანტური შემთხვევითი რიცხვის გენერატორებისა და თვითტესტირებადი QRNG-ის გაერთიანებით მივიღებთ ნახევრად თვითტესტირებად გენერატორს. ამ შემთხვევაში ჩვენ არ ვიქნებით მთლიანად დამოკიდებული მოწყობილობებზე. მოწყობილობისგან დამოუკიდებელი QRNG ხასიათდება მაღალი პროდუქტიულობითა და ეფექტურობით, ხოლო თვით ტესტირებად QRNG–ს გააჩნია სერტიფიკაციის შემთხვევითობის უფრო დიდი უსაფრთხოება.

ჩვენ გთავაზობთ ნახევრად თვით ტესტირებად QRNG-ს, რომელიც აერთიანებს თვით ტესტირებისა და მოწყობილობისგან დამოუკიდებელ QRNG-ის მისაღებ მახასიათებლებს.

თვითტესტირება კვანტურ გარემოში, რომელიც შექმნილია ერთი ფოტონის პოლარიზაციის სუპერპოზიციაში მუშაობისთვის არის

$$\psi = \frac{|H> + |V>}{\sqrt{2}}$$

ან ჩახლართულ მდგომარეობაში

$$\psi = \frac{|H>_1 |V>_2 + |V>_1 |H>_2}{\sqrt{2}}$$

კვანტური შემთხვევითი რიცხვის გენერატორი იყენებს გზის განშტოების პრინციპებს. პოლარიზატორები ფოტონს 50% ალბათობით ძლევენ უფლებას რომ გაიაროს. თეორიულად, ამ შემთხვევაში დამთხვევის მრიცხველი აღნიშნავს სრულყოფილ ანტიკორელაციას.

მოწყობილობაში არის ტესტირების ეტაპი, სადაც გაზომვების კომპლექტიდან შეყვანილი მდგომარეობის სრულ ტომოგრაფიას ხორციელდება, რათა დადგინდეს 2×2 მატრიცა,

რომელიც აღწერს ფოტონურ ორი დონის სისტემას ერთი ფოტონისთვის ან თუ გვაქვს ფოტონური წყვილის შემთხვევა, ეფექტურ ორგანზომილებიან ჰილბერტის სივრცეს. გაზომვების შედეგების მიხედვით, გენერატორი აფასებს შესაძლო მინიმალურ ენტროპიას $H_\infty(\hat{p})$, რომელიც არის მომხმარებლისა და მსმენელის საერთო მდგომარეობის მინიმალური შესაძლო ენტროპია, და $\hat{p}$ კი ყველაზე უარესია შესაძლო შედეგებში. ამის შემდეგ ბიტები გადაეცემა შემთხვევითობის ექსტრაქტორებს, რომელიც დააგენერერირებს უფრო მოკლე, მიუკერძოებელ შემთხვევით სტრიქონს ხელმისაწვდომი ენტროპიისთვის.

ეს მეთოდი გვიცავს ისეთი თავდასხმებისგან, სადაც მოწინააღმდეგეს შეუძლია გააკონტროლოს კვანტური მდგომარეობა, საიდანაც ვიღებთ ენტროპიას, მანამ სანამ არ გავაკეთებთ განმეორებით გაზომვებს ერთ მდგომარეობაზე. პირობითი ტომოგრაფიის სწორად შესასრულებლად უნდა ჩავთვალოთ, რომ გაზომილი მდგომარეობა შენარჩუნებულია მთელი პროცესის განმავლობაში. ასეთი თვითტესტირება მხოლოდ შეზღუდულ დაცვას გვთავაზობს.

ტომოგრაფია გთავაზობთ ენტროპიის შეფასებას იმ მოდელებში, სადაც განხორციელებისას მოსალოდნელია შეცდომები ან ოპერაციის დროს შეიძლება მოხდეს დარღვევები. ჩვენ ვგულისხმობთ, რომ შეცდომები არ ხდება არასანდო მწარმოებლის გამო. ეს მოდელი წარმოდგენილია თვით ტესტირებად QRNG, სადაც კვანტური შემთხვევითობის წყარო განცალკევებულია ტექნიკური ხმაურისგან dimension witness-ის გამოყენებით.

$$W = \begin{vmatrix} p(1|0,0) - p(1|1,0) & p(1|2,0) - p(1|3,0) \\ p(1|0,1) - p(1|1,1) & p(1|2,1) - p(1|3,1) \end{vmatrix}$$

თვით ტესტირებადი კვანტური შემთხვევითი რიცხვების გენერატორის პროტოკოლი შედგება ამ ნაბიჯებისაგან. პირველ რიგში, ტარდება ექსპერიმენტი, სადაც მომხმარებელი უკვე მზა მდგომარეობა x-ს და გაზომვა y, ვიღებთ შედეგს b. ამის შემდეგ, მონაცემებიდან შეიძლება გავზომოთ განაწილება p (b | x, y) და W, მოწმის მნიშვნელობის შეფასება შეგვიძლია. W იძლევა იდეას იმის შესახებ, "რამდენად კვანტურია" მომზადებისა და გაზომვების კომბინაცია. ნებისმიერი W> 0 გვიჩვენებს, რომ ზოგიერთი გაზომვა შეუთავსებელია და არსებობს გარკვეული კვანტური შემთხვევითობა, რომელიც საშუალებას იძლევა მივანიჭოთ გამოსაცნობი ალბათობა. შედეგი შეიძლება გამოყენებულ იქნას შემთხვევითობის ექსტრაქტორში შეკუმშვის დონის დასადგენად [22,23].

ალტერნატივაა გაურკვევლობის პრინციპის გამოყენება, რასი საშუალებით ნებისმიერი მოწინააღმდეგე ფლობს მხოლოდ ინფორმაციის შეზღუდულ რაოდენობას. წინა მეთოდების მსგავსად, ჩვენი მიზანი არ არის მხოლოდ შემთხვევითი ბიტების გამომუშავება, მაგრამ დარწმუნებული უნდა ვიყოთ, რომ ეს ბიტები კონფიდენციალურია (არცერთ გარე შემტევს არ შეუძლია ჩვენი თანმიმდევრობის გაგება). მაგალითად, თუ ჰორიზონტალურ ვერტიკალურ ბაზაზე ვზომავთ ფოტონის პოლარიზაციას ჩახლართულ მდგომარეობაში, მივიღებთ აბსოლუტურად შემთხვევით რიცხვებს, მაგრამ მოწინააღმდეგე, რომელსაც აქვს წვდომა ბიტების მეორე ნახევარზე, გაიგებს ზუსტ თანმიმდევრობას, რომლის მიღებაც იგივე

გაზომვებიდან შეგვიძლია. ეს შეიძლება იყოს მისაღები პროგრამებისთვის, როგორიცაა სიმულაცია, მაგრამ თავიდან უნდა იქნას აცილებული ინფორმაციის გაჟონვა კრიპტოგრაფიაში.

ჩვენ შეგვიძლია გამოვიყენოთ ბელის უტოლობების ვარიანტი, CHSH ფორმულირება. ორი მოწყობილობის გაზომვით შევისწავლით გაზომვის კორელაციებს და განვსაზღვრავთ ორ ცვლადს x და y, თითოეული თითოეული მოწყობილობისთვის. ეს ცვლადები იღებს ორ მნიშვნელობას, 0 და 1, რაც შეესაბამება ორ ორობით გაზომვას შორის არჩევანს. ორივე საზომი მოწყობილობა იდენტურია. X კონფიგურაციაში გაზომვები იძლევა a-ს ორობით მნიშვნელობას და y- ით განსაზღვრული გაზომვა იძლევა შედეგს b. ჩვენ გვაინტერესებს კორელაციის ფუნქცია, რომელიც განისაზღვრება შემდეგნაირად:

$$I = \sum_{x,y} (-1)^{x,y} [\mathrm{P}\ (\mathrm{a}\ =\ \mathrm{b} \mid \mathrm{xy}) - \mathrm{P}\ (\mathrm{a}\ \neq\ \mathrm{b} \mid \mathrm{xy})\ ]$$

სადაც P (a = b | xy) და P (a ≠ b | xy) არის ალბათობები, რომ a = b ან a ≠ b, როდესაც პარამეტრები არის x და y. რეალისტური ლოკალური თეორიისთვის ყოველთვის უნდა ვიპოვოთ I ≤ 2, რადგან ნებისმიერი მნიშვნელობა 2-ზე მეტი მიუთითებს არა ლოკალურობაზე [24].

ბელის უთანასწორობის შესაფასებლად, ეს ექსპერიმენტი უნდა ჩატარდეს n-ჯერ. თითოეული (x, y) გაზომვა წარმოიქმნება იდენტური და დამოუკიდებელი ალბათობის განაწილებით P (xy). n-ის საბოლოო გამომავალი სტრიქონი არის r = (a_1, b_1;...; a_n, b_n), და შემავალი s = (x_1, y_1;...; x_n, y_n). $\tilde{I}$ კი CHSH ფორმულის შემფასებელია, რომელიც განისაზღვრება შემდეგნაირად

$$\tilde{I} = \frac{1}{n} \sum_{x,y} (-1)^{x,y} [\mathrm{N}\ (\mathrm{a}\ =\ \mathrm{b} \mid \mathrm{xy}) - \mathrm{N}(\mathrm{a}\ \neq\ \mathrm{b} \mid \mathrm{xy})/\mathrm{P}(\mathrm{xy})\ ]$$

სადაც N (a = b, xy) არის რიცხვი, რამდენჯერ გაიზომა (x, y). შედეგები a და b აღმოჩნდა n-ის ტოლი. N (a≠B, xy) განისაზღვრება მსგავსად.

7. დასკვნა

ჩვენი ახალი კვანტური შემთხვევითი რიცხვის გენერატორის გამოყენებით შესაძლებელია ეფექტურად წარმოქმნას მეგაბიტი ან გიგაბიტი სიჩქარე. ჩვენი გენერატორი ემყარება მოსვლის დროზე დაფუძნებულ QRNG. საკმაოდ ეფექტურია, რადგან იყენებს დეტექტორების მარტივ ვერსიას, საკმაოდ მცირე მოთხოვნებით. ახალ QRNG-ს შეუძლია ერთზე მეტ შემთხვევით ბიტის გამოვლენა თითოეულ ფოტონის აღმოჩენისას.

შევისწავლეთ არასანდო მოწყობილობებთან მუშაობის კვანტური გზები. პირველად გაანალიზებულია QRNG- ის თვითტესტირების მეთოდი, შემდეგ კი მოწყობილობაზე

დამოუკიდებელი კვანტური შემთხვევითი რიცხვის გენერატორების ანალიზი. განვიხილეთ კვანტური სერტიფიკაციის სხვადასხვა ფორმები. ამ მეთოდების საფუძველზე შემოთავაზებულია კვანტური სერტიფიკაციის ახალი მეთოდი.

ეს მეთოდი შემუშავებულია მოწყობილობაზე დამოუკიდებელი გენერატორებით, რომელიც იყენებს კვანტური თეორიის სხვადასხვა ასპექტის ნაკლებად მკაცრ ექსპერიმენტულ ტესტებს, რის შედეგადაც ხდება უფრო შეზღუდული სერტიფიცირება უსაფრთხოების უფრო მოდუნებული დაშვებებით.

ბიბლიოგრაფია

1. Kabiri Chimeh, M., Heywood, P., Pennisi, M. et al. Parallelisation strategies for agent based simulation of immune systems. BMC Bioinformatics 20, 579 (2019). https://doi.org/10.1186/s12859-019-3181-y
2. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili// Novel Version of Merkle Cryptosystem// Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 4, 2017, p. 28-33
3. P. A. W. Lewis, A. S. Goodman and J. M. Miller, "A pseudo-random number generator for the System/360," in IBM Systems Journal, vol. 8, no. 2, pp. 136-146, 1969, doi: 10.1147/sj.82.0136.
4. Lambić, D., Nikolić, M. Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn 90, 223–232 (2017). https://doi.org/10.1007/s11071-017-3656-1
5. J. M. Mcginthy and A. J. Michaels, "Further Analysis of PRNG-Based Key Derivation Functions," in IEEE Access, vol. 7, pp. 95978-95986, 2019, doi: 10.1109/ACCESS.2019.2928768.
6. Herrero-Collantes, Miguel & Garcia-Escartin, Juan Carlos. (2016). Quantum Random Number Generators. Reviews of Modern Physics. 89. 10.1103/RevModPhys.89.015004.
7. High-Speed and Secure PRNG for Cryptographic Applications; T. Okhrimenko, S. Tynymbayev, M. Iavich; mecs-press.org, 2020.
8. Post-Quantum Digital Signatures with Attenuated Pulse Generator; M. Iavich, R. Bocu, A. Arakelian, G. Iashvili; ceur-ws.org, Vol-2698, 2020.
9. Improvement of Merkle Signature Scheme by Means of Optical Quantum Random Number Generators; M. Iavich, A. Gagnidze, G. Iashvili, T. Okhrimenko, A. Arakelian, A. Fesenko; Springer, 2020.
10. Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016). Quantum random number generation.
11. Michael A. Wayne and Paul G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," Opt. Express 18, 9351-9357 (2010)
12. Michael A. Wayne and Paul G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," Opt. Express 18, 9351-9357 (2010)
13. Wayne, Michael & Jeffrey, Evan & Akselrod, Gleb & Kwiat, Paul. (2009). Photon arrival time quantum random number generation. Journal of Modern Optics. 56. 516-522. 10.1080/09500340802553244.
14. Hu Z., Gnatyuk S., Okhrimenko T., Tynymbayev S., Iavich M. High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security, Issue 12 (3), pp. 1-10, 2020.
15. Gnatyuk S., Okhrimenko T., Azarenko O., Fesenko A., Berdibayev R. Experimental Study of Secure PRNG for Q-trits Quantum Crypto-graphy Protocols, Proceedings of the 2020 IEEE 11th

International Conference on Dependable Systems, Services and Technologies (DESSERT 2020), Kyiv, Ukraine, May 14, 2020, pp. 183-188.

16. Z. Hu, S. Gnatyuk, T. Okhrimenko (Zhmurko), V. Kinzeryavyy, M. Iavich, Kh. Yubuzova, High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits, CEUR Workshop Proceedings, Vol. 2393, pp. 810-821, 2019.
17. A.Gagnidze, M.Iavich, G. Iashvili, Advantages and challenges of QRNG integration into Merkle, Scientific and Practical Cyber Security Journal (SPCSJ) 4(1):93-102, 2020
18. Shrimpton T., Terashima R.S. (2015) A Provable-Security Analysis of Intel's Secure Key RNG. In: Oswald E., Fischlin M. (eds) Advances in Cryptology -- EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol 9056. Springer, Berlin, Heidelberg.
19. Gnatyuk S., Okhrimenko T., Iavich M., Berdibayev R. Intruder control mode simulation of deterministic quantum cryptography protocol for depolarized quantum channel, Proceedings of 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019, Kyiv, Ukraine, October 8-11, 2019, pp. 825-828.
20. S. Gnatyuk, T. Zhmurko, P. Falat, Efficiency Increasing Method for Quantum Secure Direct Communication Protocols, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015), Warsaw, Poland, September 24-26, Vol. 1, 2015, pp. 468-472.
21. Qoussini A.E., Daradkeh Y.I., Al Tabib S.M., Gnatyuk S., Okhrimenko T., Kinzeryavyy V. Improved model of quantum deterministic protocol implementation in channel with noise, Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2019), 2019, pp. 572-578.
22. Lunghi, Tommaso, et al. "Self-testing quantum random number generator." Physical review letters 114.15 (2015): 150501.
23. Bowles, J., Quintino, M. T., & Brunner, N. (2014). Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. Physical review letters, 112(14), 140407.
24. Pironio, S., Acín, A., Massar, S., de La Giroday, A. B., Matsukevich, D. N., Maunz, P., ... & Monroe, C. (2010). Random numbers certified by Bell's theorem. Nature, 464(7291), 1021-1024.