Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 24-34 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

THE ANALYSIS OF THE POST PROCESSING METHODS FOR THE QUANTUM RANDOM NUMBER GENERATORS

Tamari Kuchukhidze, Georgian Technical University, Scientific Cyber Security Association

ABSTRACT: Randomness is widely used in various fields including encryption, statistical analysis and numerical simulations. They are also a fundamental resource in science and engineering. For such applications, we usually need to provide unbiased and independent random bits. This raises the issue of where to get these supposed random bits.
Quantum Random Number Generators (QRNGs) generate real random numbers based on the inherent randomness of quantum measurements. In practice, unfortunately, quantum randomness is inevitably mixed with classical randomness due to classical noise. Also, randomness is often correlated and biased.
It is necessary to process the resulting raw bits sequence and convert them to good quality output values that are as close to uniform distribution as possible. Random extractors are required for this.
We will analyze the randomness obtained by quantum random number generators as well as various examples of postprocessing. We discuss the types of randomness extractors.

Keywords: *quantum, post processing, quantum random number generators, entropy, randomness extractors.*

რეზიუმე: შემთხვევითობა ფართოდ გამოიყენება სხვადასხვა სფეროში, მათ შორის დაშიფვრა, სტატისტიკური ანალიზი და რიცხვითი სიმულაციები. ისინი ასევე ფუნდამენტური რესურსია მეცნიერებასა და ინჟინერიაში. ასეთი აპლიკაციებისთვის, ჩვეულებრივ, გვჭირდება მიუკერძოებელი და დამოუკიდებელი შემთხვევითი ბიტების მიწოდება. ეს აჩენს პრობლემას, საიდან უნდა მიიღოთ ეს სავარაუდო შემთხვევითი ბიტები.
კვანტური შემთხვევითი რიცხვის გენერატორებმა (QRNG) გამოაქვთ ნამდვილი შემთხვევითი რიცხვები კვანტური გაზომვების თანდაყოლილი შემთხვევითობის საფუძველზე. პრაქტიკაში, სამწუხაროდ, კვანტური შემთხვევითობა აუცილებლად შერეულია კლასიკურ შემთხვევითობასთან კლასიკური ხმაურის გამო. ასევე შემთხვევითობა ხშირად კორელირებული და მიკერძოებულია.
აუცილებელია დავამუშავოთ მიღებულ ნედლი ბიტების თანმიმდევრობა და გარდაქმნის კარგი ხარისხის გამომავალ მნიშნელობებად, რომლებიც თანაბარ განაწილებასთან რაც შეიძლება მიახლოებულია. ამისთვის საჭიროა შემთხვევითობის ექსტრაქტორები.
გავაანალიზებთ კვანტური შემთხვევითი რიცხვების გენერატორების მიერ მიღებულ შემთხვევითობას და ასევე დამუშავების სხვადასხვა მაგალითებს. განვიხილავთ შემთხვევითობის ექსტრაქტორების სახეობებს.

საკვანძო სიტყვები: *კვანტური, კვანტური შემთხვევითი რიცხვების გენერატორები, დამუშავება, ენტროპია, შემთხვევითობის ექსტრაქტორები.*

1. შესავალი

შემთხვევითი რიცხვები გადამწყვეტ როლს თამაშობს მეცნიერების, ტექნოლოგიებისა და მრეწველობის ბევრ სფეროში, მაგალითად, კრიპტოგრაფიაში, სტატისტიკაში, სამეცნიერო სიმულაციასა და ლატარიაში [1-5]. 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 [6-8]. ფსევდო შემთხვევითი რიცხვების გენერატორები, რომლებიც ემყარება გამოთვლით სირთულეებს, კარგად განვითარდა ბოლო რამდენიმე ათწლეულის განმავლობაში და შეუძლიათ წარმოქმნან შემთხვევითი რიცხვები მაღალი სიჩქარით, მცირე რესურსების გამოყენებით. თუმცა, ფსევდო შემთხვევითი რიცხვების გენერატორების მთავარი ნაკლი არის, რომ ჩვენს მიერ მიღებული შემთხვევითობა არ არის ინფორმაცი-თეორიულად დასაბუთებადი. სინამდვილეში, ყველა პროგრამაზე დაფუძნებული ფსევდო შემთხვევითი რიცხვების გენერატორი შეიძლება განხორციელდეს დეტერმინისტული ალგორითმით, თუკი გავითვალისწინებთ საკმარის გამოთვლით სიმძლავრეს. ეს ფსევდო შემთხვევითობა გამოიწვევს პრობლემებს ბევრ გამოყენებაში, როგორიცაა კრიპტოგრაფია.

ფსევდო შემთხვევითი გენერატორების მიერ შექმნილი უსაფრთხოების პრობლემების გადასაჭრელად შეიქმნა ფიზიკური RNG-ები. კერძოდ, კვანტური მექანიკის ალბათური ბუნება გვთავაზობს ბუნებრივ გზას ინფორმაცია-თეორიულად დამტკიცებადი შემთხვევითი რიცხვების გენერატორების, კვანტური შემთხვევითი რიცხვების გენერატორების (QRNG) შესაქმნელად. საგულისხმოა, რომ ზოგიერთი ფიზიკური RNG შედის მიკროპროცესორებში, თუმცა წარმოქმნილი შემთხვევითობა არ არის კვანტური მექანიკური ხასიათის [9].

თეორიულად, QRNG-ს შეუძლია გამოიმუშავოს შემთხვევითი რიცხვები დასაბუთებადი შემთხვევითობით. პრაქტიკაში კი არ არის ასე, კვანტური სიგნალები (ჩვენთვის ჭეშმარიტი შემთხვევითობის წყარო) აუცილებლად შერეულია კლასიკურ ხმაურთან. ზოგადად, მოწინააღმდეგეს შეუძლია დაარეგულიროს კლასიკური ხმაური და მიიღოს ნაწილობრივი ინფორმაცია შემთხვევითი რიცხვების შესახებ. აქედან გამომდინარე, აუცილებელია გამოვიყენოთ შემდგომი დამუშავების პროცედურა, რათა გამოვავლინოთ ჭეშმარიტი შემთხვევითობა, რომლის შესახებაც ჩვენს მოწინააღმდეგეს თითქმის არ აქვს ინფორმაცია. ამ პროცედურას ეწოდება შემთხვევითობის მოპოვება (randomness extraction), რომელიც ხორციელდება შემთხვევითი ექსტრაქტორების გამოყენებით. სხვა სიტყვებით რომ ვთქვათ, შემთხვევითობის ექსტრაქტორები გამოიყენება ჭეშმარიტი შემთხვევითობის ამოღებისთვის და კლასიკური ხმაურის ეფექტების აღმოსაფხვრელად.

2. დამუშავების ეტაპი

სტანდარტული შემთხვევითი რიცხვის გენერატორები შექმნილია თანაბარი შემთხვევითი სტრინგის წარმოებისთვის. დამუშავების შემდგომი ეტაპი კი ამუშავებს მიღებულ ნედლი

ბიტების თანმიმდევრობას და გარდაქმნის კარგი ხარისხის გამომავალ მნიშნელობებად, რომლებიც თანაბარ განაწილებასთან რაც შეიძლება მიახლოებულია. დამუშავების პერიოდი შეიძლება მოიცავდეს ისეთ ამოცანებს, რომლებიც შეამოწმებენ გენერატორი მუშაობს თუ არა გამართულად ან ხდება საცდელი მნიშვნელობების გენერაცია, სანამ დავაგენერირებთ საბოლოო სტრინგებს [10].

გარდა ამ ამოცანებისა, რომლებიც სხვადასხვა გენერატორისთვის განსხვავებულია, დამუშავების შემდგომი ეტაპის მთავარი მიზანია შემთხვევითობის მოპოვება. ფიზიკური RNGs-ის უმეტესობა შეიცავს რომელიმე ფორმის შემთხვევითობის ექსტრაქტორს, მიკერძოებისა და კორელაციების გასასწორებლად. ისინი ჩნდება გაზომვისა და გენერაციის მოწყობილობების არასრულყოფილებით, თუნდაც გვქონდეს კარგი შემთხვევითობის წყაროები, მაღალი ენტროპიით.

მაღალი ენტროპია არ არის გარანტია იმისა, რომ წარმოქმნილი შემთხვევითი თანმიმდევრობა შესაფერისი იქნება ნებისმიერ შემთხვევაში. მიუხედავად იმისა, რომ არსებობს მეთოდები, რომლებსაც შეუძლიათ რანდომიზირებულ ალგორითმებში გამოსაყენებლად დააფიქსიროონ სუსტი წყაროები, ყველა პროტოკოლი ვერ მუშაობს არასრულყოფილ შემთხვევითობაში. კერძოდ, ბევრი კრიპტოგრაფიული პროტოკოლი ისეთი ამოცანებისთვის, როგორიცაა: ბიტების ვალდებულება, დაშიფვრა, ნულოვანი ცოდნა ან საიდუმლო გაზიარება არ არის უსაფრთხო თუ არ ვიყენებთ თითქმის თანაბარ შემთხვევით მიმდევრობას.

ზოგიერთი აპარატურული შემთხვევითი რიცხვების გენერატორი ერთმანეთში ურევს შემთხვევითობის სხვადასხვა წყაროებს, მათი ბიტების ლოგიკური XOR-ის აღებით ან კრიპტოგრაფიულ ჰეშირების ფუნქციას აწვდის სტრინგებს. ფონ ნოიმანმა შემოგვთავაზა მარტივი მიკერძოების მოშორების მეთოდი, რომლის დროსაც, წარმოქმნილი თითოეული ბიტის წყვილისთვის, შეგვიძლია გავაუქმოთ 00 და 11 შედეგები, მივანიჭოთ 01-ს 0 და 10-ს კი 1. თუკი გვაქვს სისტემური მიკერძოება, ეს მეთოდი ამოიღებს ამ მიკერძოებას, მაგრამ მინიმუმ ნახევრი ბიტების გადაგდების ხარჯზე და ბიტების სიჩქარე ერთი მეოთხედით მაინც შემცირდება (რაც უფრო მეტი ბიტს გადავაგდებთ, მით უფრო მიკერძოებული იყო ორიგინალი მიმდევრობა). ეს ძირითადი მეთოდი, რა თქმა უნდა, დაიხვეწა და უფრო ეფექტური გახდა [11].

სანამ შემთხვევითობის ექსტრაქციას განვიხილავთ უფრო დეტალურად, პირველ რიგში მნიშვნელოვანია განვსაზღვროთ რა არის ჩვენთვის მისაღები თანაბარი შედეგი. ჩვენთვის მნიშვნელოვანი ცნებაა მანძილი განაწილებებს შორის. ორი X და Y განაწილებების ალბათობა, განსაზღვრული ერთსა და იმავე მხარდაჭერაში (მათ შეუძლიათ მიიღონ იგივე მნიშვნელობები სასრულ ანბან A-ში), რომელიც შეგვიძლია განვსაზღვროთ სტატისტიკური მანძილით

$$dis(X,Y) = \max_{a \in A} |Pr_X(a) - Pr_Y(a)|$$

ეს მეტრიკა გვაძლევს მაქსიმალურ განსხვავებას კონკრეტული შედეგის მიღების ალბათობისას, შედარებით განაწილებებში. ვიტყვით, რომ ორი X და Y განაწილება არის ϵ-ახლო, თუკი

$$dis(X,Y) \leq \epsilon$$

შემთხვევითობის ექსტრაქციის მიზანია, მივიღოთ მიმდევრობა, რომელიც რაც შეიძლება ახლოს იყოს თანაბართან. ეს ჩვეულებრივ ნიშნავს, დაუმუშავებელი გამომავალი მნიშვნელობებიდან ავიღოთ n ბიტი და გარდავქმნათ m ბიტების სტრინგად, რომლის განაწილება ϵ-ახლოა U_m-თან ($\{0, 1\}^m$-ში არის თანაბარი განაწილება) მცირე ϵ-სთვის, რომელიც დამოკიდებულია ჩვენ საჭიროებებზე.

იდეალურ შემთხვევაში, ჩვენ გვსურს ექსტრაქტორები, რომლებიც მოგვცემს რაც შეიძლება მეტ გამომავალ ბიტს, მცირე დამატებითი რესურსების გამოყენებით, როგორიცაა გამოთვლის დრო ან დამატებითი შემთხვევითობა. ნედლი მიმდევრობის განაწილების მინიმალური ენტროპია გვაძლევს ზღვარს რამდენი ბიტის ამოღებაა შესაძლებელი. თუ ჩვენ ავიღებთ n ბიტიან სტრინგს ნედლი მიმდევრობიდან, რომელსაც X განაწილებით $H_\infty(X) = k$ მინიმალური ენტროპია გააჩნია, შეგვიძლია ამოვიღოთ მაქსიმუმ k შემთხვევითი ბიტი, რომელიც თანაბართან ახლოსაა. ორიგინალ სიგრძეს არ აქვს მნიშვნელობა. შემთხვევით წყაროს ეწოდება (n, k)-წყარო, თუ ის აწარმოებს n ბიტს $H_\infty(X) = k$ მინიმალური ენტროპიით, X განაწილებიდან.

განვიხილავთ ბიტების თანმიმდევრობის გენერაციის სხვადასხვა მეთოდებს, რომლებიც თანაბართან მიახლოებულ მიმდევრობას გვაძლევენ, მინიმალურ ენტროპიის ზღვართან ახლოს. ასევე განვიხილავთ სხვადასხვა შემთხვევითობის ექსტრაქტორების მიდგომების უპირატესობებსა და შეზღუდვებს.

3. შემთხვევითობის ექსტრაქტორები

შემთხვევითობის ექსტრაქტორები ფუნქციებია, რომლებიც ამოიღებენ თითქმის ერთგვაროვან ბიტებს მიკერძოებული და კორელირებული ბიტების წყაროებიდან. ისინი ენტროპიის სუსტ წყაროს თანაბარი ბიტების გენერატორად გადააქცევენ. ეს ფუნქციები თავიდან შემოიტანეს რანდომიზირებული ალგორითმების შესასწავლად, მაგრამ გახდა ძირითადი ინსტუმენტი თეორიული კომპიუტერული მეცნიერების მრავალ სფეროში. შემთხვევითობის ექსტრაქტორებს და მასთან დაკავშირებული ცნებებს, როგორიცაა დისპერსიები, კონდენსატორები და გაფართოების გრაფიკები, სხვადასხვა გამოყენება გააჩნია და ფსევდო შემთხვევითი რიცხვების გენერატორების მრავალ სფეროში გვხვდება, მათ შორის, შეცდომის გამოსწორების კოდებში, სინჯები, გაფართოების გრაფიკები და სიხისტის გამაძლიერებლები.

განვიხილავთ QRNG–სთვის ყველაზე შესაფერისი ექსტრაქტორების რამდენიმე ცნებას. შემთხვევითობის მოპოვების მრავალი ვარიანტი არსებობს და საბოლოო არჩევანზე გავლენას ახდენს თითოეული მეთოდის სიჩქარე და ტექნიკა. იმისათვის, რომ ეფექტური მეთოდი გვქონდეს და რაც შეიძლება მეტი ბიტი შევინარჩუნოთ, საჭიროა კარგად განვსაზღვროთ ჩვენთვის ხელმისაწვდომი ენტროპია და შემდეგ ავირჩიოთ ადეკვატური შემთხვევითობის ექსტრაქტორი. წინააღმდეგ შემთხვევაში, ექსტრაქტორის ფუნქციის გამომავალ მნიშვნელობებს არ ექნებათ სასურველი თვისებები.

შემდეგში, ჩვენ ჩავთვლით, რომ გვაქვს კარგად აღწერილი შემთხვევითობის წყარო. ვვარაუდობთ, რომ დაუმუშავებელ მიმდევრობას აქვს ნაცნობი მინიმალური ენტროპია ან ზოგიერთ შემთხვევაში, ისეთი ცნობილი თვისებები მაინც, როგორიცაა ბიტებს შორის დამოუკიდებლობა ან რომ ეს მიმდევრობა გამომდინარეობს მარკოვის პროცესიდან.

ჩვენ ასევე ჩავთვლით, რომ სტანდარტულად გვსურს (n, m, k, ϵ) - ექსტრაქტორი: ფუნქცია, რომელიც გარდაქმნის (n, k) - წყაროს n ბიტს m გამომავალ ბიტებად, რომლის განაწილება ϵ-ახლოსაა თანაბართან, ხოლო m რაც შეიძლება ახლოსაა k-სთან.

4. დეტერმინისტული ექსტრაქტორები

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.

დეტერმინისტული ექსტრაქტორები ფუნქციებია

$$Ext: \{0,1\}^n \rightarrow \{0,1\}^m$$

რომლებიც იღებს n ბიტების $\{0, 1\}^n$ შემავალ სტრინგებს და გვაძლევს m გამომავალ ბიტებს. ეს ფუნქციები განსაკუთრებით მიმზიდველია, რადგან დეტერმინისტული ალგორითმებია, რომლებსაც მუშაობისთვის მხოლოდ შემავალი თანმიმდევრობა სჭირდება. თუმცა, აქვთ გარკვეული შეზღუდვები, რომლებიც ხელს უშლის მათ გამოყენებას შემთხვევითობის გარკვეულ წყაროებში.

ელემენტარული არგუმენტი გვიჩვენებს, რომ შეუძლებელია ზოგადი დეტერმინისტული ექსტრაქტორები. წარმოვიდგინოთ ფუნქცია $\{0, 1\}^n$-დან $\{0, 1\}$. შეგვიძლია გამოვყოთ ყველა შესაძლო შემავალი მნიშვნელობების n ბიტიანი სტრიქონი ერთ ნაკრებში, რომელიც გვაძლევს 0 მნიშვნელობას, $Ext^{-1}(0)$, და გვექნება მეორე ნაკრები, რომელიც გვაძლევს 1-ს, $Ext^{-1}(1)$. მინიმუმ ერთ-ერთს მაინც აქვს 2^{n-1} ან მეტი ზომა. შემავალ მნიშვნელობას, რომელიც წარმოადგენს თანაბარ განაწილებას უფრო დიდ ნაკრებში, გააჩნია $n-1$ მინიმალური ენტროპია მაინც, მაგრამ ყოველთვის გვაძლევს ერთი და იგივე გამომავალ მნიშვნელობებს,

რაც გვიჩვენებს, რომ არ არსებობს ერთი ზომის ექსტრაქტორი, რომელიც ვალიდურია ნებისმიერი შემავალი განაწილებისთვის.

თუმცა, არსებობს მოქმედი ექსტრაქტორები, პროცესების გარკვეულ ოჯახების შემავალი განაწილებებისთვის, რომლებიც მიეკუთვნებიან პროცესების გარკვეულ ოჯახებს და აღწერენ გონივრულ წყაროებს. სხვათა შორის, არსებობს პრაქტიკული დეტერმინული ექსტრაქტორები შერჩევითი განაწილებისთვის, ბიტების ფიქსირებული წყაროებისთვის, სადაც მოწინააღმდეგეს შეუძლია დააყენოს ბიტების ნაწილი და განზოგადოება აფინური წყაროებისთვის ან წყაროები, ისეთი გამომავალი მნიშვნელობებით, რომლებიც თანაბრადაა განაწილებული უცნობ ალგებრულ ნაირსახეობაზე.

ცვლადი სიგრძის დეტერმინისტული ექსტრაქტორები ქმნიან საინტერესო დეტერმინისტული ექსტრაქტორების კიდევ ერთ ჯგუფს, რომლებიც ოდნავ გადაიხრება დეტერმინისტული ექსტრაქტორის მოცემული განმარტებიდან. ეს ნაჩვენებია ფონ ნოიმანის ალგორითმში: დეტერმინისტული მეთოდი, რომელიც მუშაობს უცნობი განაწილებისთვის და გვაძლევს სიგრძის გამომავალ მნიშვნელობას, რომელიც არ არის ცნობილი ექსტრაქციამდე.

ფონ ნოიმანმა შემოგვთავაზა მეთოდი, რომლის დროსაც, წარმოქმნილი თითოეული ბიტის წყვილისთვის, შეგვიძლია გავაუქმოთ 00 და 11 შედეგები, მივანიჭოთ 01-ს 0 და 10-ს კი 1.

აღწერილი ფონ ნოიმანის შემთხვევითობის ექსტრაქტორის ერთადერთი აუცილებელი პირობაა, რომ თითოეული შემავალი ბიტი იყოს დამოუკიდებელი წინა და მის შემდგომი ბიტებისგან. ფონ ნოიმანის მეთოდის დახვეწილი ვერსიები ამცირებენ გადაყრილ ენტროპიას და გვაძლებს ეფექტურობას ინფორმაციის თეორიის ზღვართან ახლოს, რომელიც მოცემულულია წყაროს შანონის ენტროპიით. შემდგომი ცვლილებების შედეგად მივიღეთ ალგორითმები, რომლებიც აწარმოებენ მიუკერძოებელ მიმდევრობებს უფრო ზოგადი პირობებით, შეყვანის თანმიმდევრობა მოდის მარკოვის ჯაჭვიდან.

ორიგინალი მეთოდის მთავარი მომხიბვლელობა მისი სიმარტივეა. ის მოითხოვს მინიმალურ გამოთვლით ენერგიას. ის შეძლება განხორციელდეს მხოლოდ ძირითადი აპარატურით და წყაროზე განაწილების სრულყოფილად ცნობა არ არის აუცილებელი. თუმცა, ორიგინალ მეთოდს გააჩნია რამდენიმე მნიშვნელოვანი შეზღუდვა. თუ ჩვენ გვყავს გარე შემტევი, რომელსაც შეუძლია მიკერძოების შეცვლა ბიტიდან ბიტზე, თუნდაც მცირედით, ფონ ნოიმანის ექსტრაქტორი აღარ იმუშავებს. სინამდვილეში, არ არსებობს დეტერმინისტული ალგორითმი, რომელიც $X = (X_1, X_2, \dots, X_n)$ ცვლადისთვის n ბიტით მოგვცემს თანაბარ გამომავალ მნიშვნელობას, თუ შეყვანილი ბიტების მიკერძოება იცვლება ისე, რომ 1-ის პოვნის ალბათობა მე-n ბიტისთვის დამოკიდებულია წინა ბიტის s მნიშვნელობის გაზომილ სტრინგზე

$$\delta \leq P_{X_i}(1|x_1 x_2 \dots x_{n-1} = s) \leq 1 - \delta$$

$0 < \delta \leq \frac{1}{2}$ -სთვის. ამას Santha-Vazirani-ის წყაროს უწოდებენ. აღწერილია სუსტი შემთხვევითობის წყაროების მოდელი დეტერმინისტული ექსტრაქტორის შეუძლებლობის მტკიცებულებასთან.

ამ შეზღუდვის მიუხედავად, არსებობს დეტერმინისტული ალგორითმები, რომლებიც საშუალებას გვაძლევს გამოვიყენოთ სუსტი Santha-Vazirani-ის წყარო, შემთხვევითი ალგორითმების სიმულაციისთვის. რანდომიზაციის მოთხოვნები ნაკლებად მკაცრია, ვიდრე სხვა გამოყენებისთვის, როგორიცაა კრიპტოგრაფია. ზოგჯერ სუსტი წყაროები, რომლებიც ვერ ახერხებენ თითქმის ერთნაირი შედეგების გამომუშავებას, ზოგიერთ შემთხვევაში მართებულია.

მაშინაც კი, თუ ჩვენ ვიყენებთ დეტერმინისტულ ექსტრაქტორს, ერთი სუსტი წყარო არ არის საკმარისი მრავალი კრიპტოგრაფიული პროტოკოლისთვის. მიუხედავად იმისა, რომ სუსტი შემთხვევითობა შეიძლება უსაფრთხოდ გამოვიყენოთ ხელმოწერის სქემებში, დაშიფვრასა და მასთან დაკავშირებულ სხვა პროტოკოლებში მაღალი ხარისხის გასაღებია საჭირო, სხვა შემთხვევაში ისინი გახდებიან დაუცველები.

მოწყობილობებისთვის, სადაც აუცილებელია გამომავალი მნიშვნელობები თანაბართან იყოს ახლოს, არსებობს მარტივი გადაწყვეტა. გავაერთიანოთ ორი, დამოუკიდებელი, სუსტი Santha-Vazirani წყაროს შედეგები, რათა გამოვიტანოთ გამომავალი მიმდევრობა, რომელსაც ვერ გამოვარჩევთ პოლინომიური დროის ალგორითმით თანაბარი განაწილებიდან. სანამ გვაქვს წვდომა ფიზიკურ მეთოდზე, რომელიც გარკვეულ შემთხვევითობას წარმოქმნის, შეგვიძლია დავაგენერიროთ ბიტის სტრინგები, რომლებსაც ვერ გამოვარჩევთ შემთხვევითი სტრინგებისგან ნებისმიერი ეფექტური ალგორითმით. ეს ისეთივე კარგია, როგორც ჭეშმარიტი შემთხვევითობა შემთხვევითობის ბევრ იმპლემენტაციაში, მათ შორის კრიპტოგრაფიაში.

აქამდე საუბარი იყო ერთი წყაროს ექსტრაქტორებზე. მრავალი წყაროს ექსტრაქტორები მისდევენ ამ მოდელს და იღებენ შედეგს ორი ან მეტი სუსტი წყაროდან. ამუშავებენ მათ და წარმოიქმნება მიმდევრობა, რომელიც თანაბართან არის მიახლოებული. არსებობს ბევრი მეთოდი, რომელიც დამოკიდებულია კონკრეტული შემავალი მნიშვნელობების განაწილებაზე, წყაროების რაოდენობაზე და გამომავალი მიმდევრობის სასურველ თვისებებზე.

წყაროების შერწყმა ასევე გამოიყენება შემთხვევითობის ექსტრაქტორების მეორე მთავარ ჯგუფში, თესლიან ექსტრაქტორებში (seeded extractors). ისინი შეგვიძლია წარმოვიდგინოთ მრავალი წყაროს ექსტრაქტორების სპეციალური შემთხვევა, ერთი სუსტი წყაროსა და იდეალურად თანაბარი წყაროთი, რომელიც წარმოქმნის მხოლოდ მცირე ოდენობის ბიტებს.

5. თესლიანი ექსტრაქტორები

როგორც ვნახეთ, ბევრი ნედლი ბიტის განაწილებისთვის, შეგვიძლია მივაღწიოთ მხოლოდ თანაბარ შედეგს, მხოლოდ რაიმე დამატებითი შემთხვევითობის დახმარებით. თესლიან ექსტრაქტორებში კი გვაქვს ფუნქცია

$$Ext: \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

ამ ფუნქციაში შედის n ბიტები ნედლი მიმდევრობა, d თანაბარი შემთხვევითი თესლის ბიტები, ხოლო წარმოიქმნება m გამომავალი ბიტები. ვთვლით, რომ d გაცილებით მცირეა, ვიდრე m. თესლის დამატებით, გვაქვს იმის გარანტია, რომ არსებობს ექსტრაქტორები, რომლებიც წარმოქმნიან თითქმის თანაბარ გამომავალ მნიშვნელობებს, რომლის სიგრძე მიახლოებულია მაქსიმალურ სიგრძესთან. ეს თესლი მსგავს როლს თამაშობს, როგორც თესლი, ფსევდო შემთხვევითი რიცხვების გენერატორებში. (k, ϵ) ექსტრაქტორს ვუწოდებთ ფუნქციას, ნებისმიერი k შემავალი წყაროსთვის (ნედლი მიმდევრობა, მინიმალური ენტროპია k მაინც), რომელიც წარმოქმნის გამომავალ თანმიმდევრობას, რომელიც ϵ-თი ახლოსაა თანაბართან. თესლი მოქმედებს, როგორც კატალიზატორი, რომელიც საშუალებას გვაძლევს ვიპოვოთ ზოგადი მეთოდები, რომლებიც ყოველთვის იმუშავებს.

შემთხვევითობის თესლიანი ექსტრაქტორები პირველად განისაზღვრა შემთხვევითი ალგორითმების კონტექსტში. ალბათური მეთოდების გამოყენებით, ნაჩვენებია, რომ ყოველთვის არსებობს ექსტრაქტორები, რომლებიც მოიცავს თითქმის ყველა არსებულ ფარულ ენტროპიას, შეყვანილი k წყაროს ნედლ თანმიმდევრობიდან. k წყაროს n ბიტების ბლოკების შესაყვანად, შეგვიძლია ავაწყოთ ექსტრაქტორები $m \approx k + d$ ზომის, რომელიც ϵ-თი ახლოსაა თანაბართან, გამოიყენება d სიგრძის თესლი $\log_2 n$. ამ თესლიანი ექსტრაქტორებისთვის არსებობს სხვადასხვა კონსტრუქციები.

თანაბარი თესლის საჭიროება, როგორც ჩანს, წინააღმდეგობრივია: ჩვენ გვჭირდება რესურსი, რომლის წარმოებასაც ვცდილობთ. თუმცა, თესლზე რეკვიზიტები ნაკლებად შემზღუდველია, ვიდრე ჩანს. ბევრ აშკარა ექსტრაქტორში თესლის სიგრძის ზომა ლოგარითმულია შემავალი სტრინგის ზომის. საკმარისად მცირე d- სთვის, შეგვიძლია შეცვალოთ შემთხვევითობის აუცილებელი მოთხოვნა ყველა 2^d შესაძლო თანმიმდევრობით. რანდომიზებულ ალგორითმებში, ანგარიშს, რომელსაც მოსდევს უმრავლესობის ხმის მიცემის ნებართვები, კარგია თანაბარი წყაროს სიმულაციისთვის. თუმცა, ეს მიდგომა აშკარად არ არის ვალიდური კრიპტოგრაფიისთვის, სადაც ჩვენ გვჭირდება არაპროგნოზირებადობა. კვანტური შემთხვევითი რიცხვის გენერატორებში, თესლიანი ექსტრაქტორები გვიცავს გარე თავდამსხმელებისგან. არსებობს კონსტრუქციები, რომელთათვისაც არსებობს უსაფრთხოების მტკიცებულებები, სხვადასხვა ძალის კვანტური თავდამსხმელების წინააღმდეგ.

პირველი თვალსაჩინო შედეგია Trevisan- ის ექსტრაქტორი. მნიშვნელოვანი თეორიული ინტერესი გამოიწვია მან მისი მონაცემების სიმცირის გამო, არამედ განსაკუთრებით იმიტომ, რომ ის უსაფრთხოა კვანტური მოწინააღმდეგეებისგან [12]. ტრევიზანის ექსტრაქტორის

თესლის სიგრძე შემავალი მნიშვნელობის სიგრძის პოლიგარითმულია და ასევე შეიძლება დადასტურდეს, რომ ის არის ძლიერი ექსტრაქტორი [13]. ანუ, ტრევიზანის ექსტრაქტორის შემთხვევითი თესლი შეიძლება ხელახლა გამოვიყენოთ. ეს განსაკუთრებით მნიშვნელოვანია პოპულარული უნივერსალური ჰეშინგის ფუნქციებისთვის, მაგალითად Toeplitz hashing.

ტრევიზანის ექსტრაქტორი აგებულია Nisan-Widgerson-ის ფსევდო შემთხვევითი რიცხვების გენერატორზე. ეს შეიძლება ჩაითვალოს, როგორც შემთხვევითი ფუნქცია, რომლის ჭეშმარიტობის ცხრილი მოცემულია ბიტების სუსტი წყაროდან. შემთხვევითი ფუნქცია აფართოებს თანაბარი შემთხვევითი თესლია d ბიტებს, როგორც PRNG, ისე ექსტრაქტორის მნიშვნელობით. ტრევიზანის ექსტრაქტორის სხვადასხვა ვარიაციები განხორციელდა კვანტური შემთხვევითი რიცხვების გენერატორებით და კვანტურ გასაღების განაწილებაში. მათი მთავარი უპირატესობა არის ის, რომ შემთხვევითი, თანაბარი თესლის ზომა მხოლოდ პოლი-ლოგარითმულია შეყვანის ბლოკების ზომის. თუმცა, პრაქტიკულმა იმპლემენტაციამ შეიძლება შეანელოს ბიტების გენერაციის პროცესი, რადგან ექსტრაქციის დროს საჭიროა გამოთვლები.

მეორე ზოგადი მეთოდია ორი უნივერსალური ჰეშირება (two-universal hashing). The Leftover Hash Lemma გვიჩვენებს, რომ ორი უნივერსალური ჰეშირების ფუნქცია, საკმაოდ მაღალი ენტროპიის შეყვანილი მნიშვნელობებით, თითქმის თანაბრად შემთხვევითია [14]. ორი უნივერსალური ჰეშირების ფუნქციებს, შეუძლია შემთხვევითობის ამოღება სუსტ წყაროში, საიმედოდ, ჯაშუშის თანდასწრებით. თუ ჩვენ გვაქვს კარგი შეფასება ან ჩვენი სუსტი შემთხვევითი წყაროს კორელაციაზე კონსერვატიული შეზღუდვა მომსმენთან, პირობითი ენტროპიების გამოყენებით შესაძლებელია გამოვიყენოთ ლემას განზოგადება, გვერდითი ინფორმაციის გამოყენებით [15]. ფართო გაგებით, გვერდითი ინფორმაციაც შეიძლება იყოს კვანტური. კვანტური შემთხვევითი რიცხვების გენერატორში სადაც არის ტექნიკური ხმაური შეგვიძლია ვივარაუდოთ, რომ ყველა შემთხვევითობა, რომელიც არასრულყოფილებისგან მოდის, ან სხვაგვარად არ ეგუება კვანტური სისტემის ჩვენს მოდელს, რომელიც აწარმოებს ნედლეულ ბიტს, არის ჯაშუშის გამო. ამ პირობებში ჯერ კიდევ შესაძლებელია თესლიანი ექსტრაქტორის შემუშავება, რომელიც იძლევა თითქმის თანაბარ შედეგს, რომელიც დამოუკიდებელია გარე სისტემებისგან. ეს მეთოდები ასევე გამოიყენება კვანტური გასაღების განაწილებაში, კონფიდენციალურობის გაძლიერების დროს.

შემთხვევითობის ექსტრაქტორი ორი უნივერსალური ან უფრო ზოგადად I-უნივერსალური ჰეშირებით გვაიძულებს გამოვიყენოთ შედარებით გრძელი თესლი, რომელიც ეკვივალენტურია n ბლოკის ზომის, მაგრამ მისი გადამუშავება შესაძლებელია. ასევე შემთხვევითად შერჩეული თანაბარი თესლის ხელმეორედ გამოყენება შესაძლებელია.

ტრევიზანის ექსტრაქტორის დანერგვისგან განსხვავებით, ეს მეთოდი გვთავაზობს სწრაფი ამოღების ფუნქციას, რომელიც იყენებს ნაკლებ გამოთვლით რესურსებს, უფრო დიდი თესლის ხარჯზე. ზოგიერთი იმპლემენტაცია, მაგალითად, Toeplitz–ის შემთხვევითი ორობითი მატრიცებით ჰეშირება, განსაკუთრებით ეფექტურია. შეგვიძლია განვსაზღვროთ ერთი ასეთი ექსტრაქტორი, სადაც თესლი გამოიყენება როგორც მართკუთხა მატრიცა,

რომელიც მრავლდება n- ვექტორებზე წყაროდან და წარმოქმნის თითქმის დამოუკიდებელ ბიტებს. ეს მიდგომა გამოიყენება ზოგიერთ კომერციულ მოწყობილობაში, რომლებიც შეიცავს ექსტრაქციის ფუნქციას, როგორც წინასწარ გამოთვლილ შემთხვევით მატრიცა, რომელიც ასრულებს თესლის როლს და გადანაწილებულია მოწყობილობაში კოდირებულად. მიუხედავად იმისა, რომ თესლის მაღალი ხარისხის შემთხვევითობა რთული პროცესია, ამის გაკეთება მხოლოდ ერთხელაა საჭირო. გრძელი არადახვეწილი მეთოდები, როგორებიცაა მრავალჯერადი დამოუკიდებელი გენერატორის XOR– ის განმეორებით აღება, მისაღებია.

ბიბლიოგრაფია

1. M. Iavich, T. Kuchukhidze, T. Okhrimenko and S. Dorozhynskyi, "Novel Quantum Random Number Generator for Cryptographical Applications," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 727-732, doi: 10.1109/PICST51311.2020.9467951.
2. M. Iavich, T. Kuchukhidze, T. Okhrimenko and S. Dorozhynskyi, "Novel Quantum Random Number Generator for Cryptographical Applications," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 727-732, doi: 10.1109/PICST51311.2020.9467951.
3. E. Jintcharadze and M. Iavich, "Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems," *2020 IEEE East-West Design & Test Symposium (EWDTS)*, 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.
4. 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
5. 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
6. 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.
7. 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
8. 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.
9. Ma, Xiongfeng, Feihu Xu, He Xu, Xiaoqing Tan, Bing Qi, and Hoi-Kwong Lo. "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction." Physical Review A 87, no. 6 (2013): 062327.
10. Herrero-Collantes, Miguel & Garcia-Escartin, Juan Carlos. (2016). Quantum Random Number Generators. Reviews of Modern Physics. 89. 10.1103/RevModPhys.89.015004.
11. Rožić, Vladimir, Bohan Yang, Wim Dehaene, and Ingrid Verbauwhede. "Iterating von Neumann's post-processing under hardware constraints." In 2016 IEEE international symposium on hardware oriented security and trust (HOST), pp. 37-42. IEEE, 2016.
12. De, Anindya, Christopher Portmann, Thomas Vidick, and Renato Renner. "Trevisan's extractor in the presence of quantum side information." SIAM Journal on Computing 41, no. 4 (2012): 915-940.

13. Raz, Ran, Omer Reingold, and Salil Vadhan. "Extracting all the randomness and reducing the error in Trevisan's extractors." Journal of Computer and System Sciences 65, no. 1 (2002): 97-128.
14. Stinson, Douglas Robert. Universal hash families and the leftover hash lemma, and applications to cryptography and computing. Faculty of Mathematics, University of Waterloo, 2001.
15. Tsurumaru, Toyohiro, and Masahito Hayashi. "Dual universality of hash functions and its applications to quantum cryptography." IEEE transactions on information theory 59, no. 7 (2013): 4700-4717.