Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 93 – 102 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ADVANTAGES AND CHALLENGES OF QRNG INTEGRATION INTO MERKLE

Maksim Iavich[1], Tamuna Kuchukhidze[2], Avtandil Gagnidze[3], Giorgi Iashvili[1]
[1]Caucasus University, Scientific Cyber Security Association, Tbilisi, Georgia
[2] Georgian Technical University, Scientific Cyber Security Association
[3]Scientific Cyber Security Association

ABSTRACT. Google Corporation, NASA and the Universities Space Research Association have teamed up with D-Wave, the manufacturer of quantum processors. Quantum computers will be able to break most, if not absolutely all conventional cryptosystems, that are widely used in practice, for example RSA. RSA cryptosystem is used in different products on different platforms and in different areas. To date, this cryptosystem is integrated into many commercial products, the number of which is growing every day.

Hash-based digital signature schemes offer an alternative. Like any other digital signature scheme, hash-based digital signature schemes use a cryptographic hash function. Their security relies on the collision resistance of that hash function.

In 1979 Ralph Merkle proposed Merkle signature scheme. Merkle signature scheme has efficiency problems, so it cannot be used in practice. World scientists are working on improving the scheme. One of the improvements is integrating PRNG (pseudo random number generator) not to calculate and store large amount of one-time keys pairs. This approach cannot be considered secure, because according to our research quantum computers are able to crack PRNG, which were considered safe against attacks of classical computers.

In the article it is offered to use hash based pseudo random number generator and the quantum random number generator for generating the seed. The advantages and disadvantages of the scheme are analyzed.

Keywords: *quantum, random number generator, pseudo-random number generator, digital signature*.

რეზიუმე: გუგლის კორპორაცია, NASA და Universities Space Research Association შეუერთდა D-Wave-ს, კვანტური პროცესორების მწარმოებელს. კვანტურ კომპიუტერს შეუძლია გატეხოს უმეტესობა, შესაძლოა ყველა ტრადიციული კრიპტოსისტემა, რომლებიც პრაქტიკაში ფართოდ გამოიყენება, მაგალითად RSA. RSA კრიპტოსისტემა გამოიყენება სხვადასხვა პროდუქტებში, სხვადასხვა პლატფორმასა და განსხვავებულ სფეროებში. დღესდღეობით, ეს კრიპტოსისტემა ინტეგრირებულია ბევრ კომერციულ პროდუქტში, რომელთა რიცხვი ყოველდღიურად იზრდება.

ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემები გვთავაზობს ალტერნატივას. როგორც სხვა ნებისმიერი ციფრული ხელმოწერის სქემა,

ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემები იყენებს კრიპტოგრაფიულ ჰეშ ფუნქციას. მათი უსაფრთხოება ეყრდნობა ჰეშ ფუნქციის შეჯახების წინაღობას.
1979 წელს Ralph Merkle-მა შემოგვთავაზა Merkle-ს ხელმოწერის სქემა. Merkle-ს ხელმოწერის სქემას ეფექტურობის პრობლემა აქვს, მისი პრაქტიკაში გამოყენება არ შეიძლება. მსოფლიოს მეცნიერები მუშაობენ ამ სქემის გაუმჯობესებაზე. ერთ-ერთია PRNG-ის (ფსევდო შემთხვევითი რიცხვების გენერატორის) ინტეგრირება, რათა არ შევინახოთ გამოთვლები და დიდი ოდენობით ერთჯერადი გასაღების წყვილები. ეს მიდგომა არ არის უსაფრთხო, რადგან ჩვენი გამოკვლევების თანახმად, კვანტურ კომპიუტერებს PRNG-ის გატეხვა შეუძლიათ, რომელიც უსაფრთხოა კლასიკური კომპიუტერებიდან შეტევების შემთხვევაში.
სტატიაში შემოთავაზებულია ჰეშირებაზე დაფუძნებული ფსევდო შემთხვევითი რიცხვების გენერატორებისა და კვანტური შემთხვევითი რიცხვების გენერატორებისთვის საწყისი მნიშვენლობების გენერაცია. გაანალიზებულია სქემის დადებითი და უარყოფითი მხარეები.

საკვანძო სიტყვები: კვანტური, შემთხვევითი რიცხვების გენერატორები, ფსევდო შემთხვევითი რიცხვების გენერატორები, ციფრული ხელმოწერა.

1. შესავალი

გუგლის კორპორაცია, NASA და Universities Space Research Association შეუერთდა D-Wave-ს, კვანტური პროცესორების მწარმოებელს. კვანტურ კომპიუტერს შეუძლია გატეხოს უმეტესობა, შესაძლოა ყველა ტრადიციული კრიპტოსისტემა, რომლებიც პრაქტიკაში ფართოდ გამოიყენება, მაგალითად RSA. RSA კრიპტოსისტემა გამოიყენება სხვადასხვა პროდუქტებში, სხვადასხვა პლატფორმებზე და განსხვავებულ სფეროებში. დღესდღეობით, ეს კრიპტოსისტემა ინტეგრირებულია ბევრ კომერციულ პროდუქტში, რომელთა რიცხვი ყოველდღიურად იზრდება. RSA სისტემა ასევე ფართოდ გამოიყენება ოპერაციულ სისტემებში: Microsoft, Apple, Sun, და Novell. ტექნიკურ მოწყობილობებში RSA ალგორითმი გამოიყენება უსაფრთხო ტელეფონებში, Ethernet-ში, ქსელურ ბარათებში, სმარტ ბარათებში, ასევე ფართოდაა გავრცელებული კრიპტოგრაფიულ აპარატურაში. ამასთან, ალგორითმი წარმოადგენს დაცული ინტერნეტ კომუნიკაციების ძირითადი პროტოკოლების ნაწილს, მათ შორის S / MIME, SSL და S / WAN. ასევე გამოიყენება ბევრ ორგანიზაციაში, მაგალითად: მთავრობა, ბანკები, კორპორაციების დიდი ნაწილი, საჯარო ლაბორატორიები და უნივერსიტეტები. RSA BSAFE დაშიფვრის ტექნილოგიას მსოფლიოში საშუალოდ 500 მილიონი მომხმარებელი იყენებს. ვინაიდან დაშიფვრის ტექნოლოგიებში ძირითადად RSA ალგორითმი გამოიყენება, ის შეგვიძლია ჩავთვალოთ ყველაზე გავრცელებულ ღია გასაღების კრიპტოსისტემად, რომელიც ინტერნეტის განვითარებასთან ერთად ვითარდება. ამის საფუძველზე, RSA-ს განადგურებით ადვილი გახდება უმეტესი პროდუქტების გატეხვა, რაც სრულ ქაოსში გადაიზრდება.

1.1 ციფრული ხელმოწერები

ციფრული ხელმოწერა ინტერნეტისა და სხვა IT ინფრასტრუქტურების უსაფრთხოებაში ძირითადი ტექნოლოგიაა. მისი საშუალებით უზრუნველყოფილია მონაცემების საიმედოობა, მთლიანობა და non-repudiation. ციფრული ხელმოწერა ფართოდ გამოიყენება იდენთიფიკაციისა და აუთენტიფიკაციის პროტოკოლებში. ასე რომ, უსაფრთხო ციფრული ხელმოწერის არსებობა კიბერ უსაფრთხოებისთვის აუცილებელია. ციფრული ხელმოწერის ალგორითმები, რომლებსაც პრაქტიკაში ვიყენებთ შემდეგია: RSA, DSA და ECDSA. ისინი არ არიან კვანტურად იმუნური, რადგან მათი უსაფრთხოება ეყრდნობა დიდი შედგენილი მთელი რიცხვების დაშლის სირთულესა და დისკრეტული ალგორითმების გამოთვლას. ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემები გვთავაზობს სერიოზულ ალტერნატივას. როგორც სხვა ციფრული ხელმოწერის სქემა, ჰეშირებაზე დაფუძნებული სქემაც იყენებს კრიპტოგრაფიულ ჰეშ ფუნქციას. მათი უსაფრთხოება ამ ჰეშირების ფუნქციის შეჯახების წინაღობაზეა დამოკიდებული.

1.2 ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერები

შემოგვთავაზეს ერთჯერადი ხელმოწერის სქემა - "Lamport One-Time Signature Scheme" [1].

1.2.1 ამ სისტემის ხელმოწერის გასაღები X შეიცავს n სიგრძის 2n ხაზს, რომლებიც შემთხვევითაა შერჩეული.

$X= (x_{n-1}[0], x_{n-1}[1], \ldots, x_0[0], x_0[1]) \in \{0,1\}^{n,2n}$

სისტემის ვერიფიკაციის გასაღები Y შეიცავს n სიგრძის 2n ხაზს, რომლებიც შემთხვევითაა შერჩეული.

$Y= (y_{n-1}[0], y_{n-1}[1], \ldots, y_0[0], y_0[1]) \in \{0,1\}^{n,2n}$

გასაღების გამოსათვლელად ვიყენებთ ცალმხრივ ფუნქცია f-ს:

$f: \{0,1\}^n \rightarrow \{0,1\}^n;$

$y_i[j] = f(x_i[j]), 0<=i<=n-1, j=0,1$

1.2.2 დოკუმენტის ხელმოწერა:

თვითნებური ზომის m შეტყობინება, ჰეშ ფუნქციის საშუალებით n ზომად გადაიქცევა:

$h(m)=hash = (hash_{n-1}, \ldots , hash_0)$

h ფუნქცია კრიპტოგრაფიული ჰეშ ფუნქციაა:

$h: \{0,1\}^* \rightarrow \{0,1\}^n$

ხელმოწერა შემდეგნაირად ხდება:

$sig = (x_{n-1}[hash_{n-1}], \ldots, x_0[hash_0]) \in \{0,1\}^{n,n}$

თუკი შეტყობინების i-ური ბიტი 0-ის ტოლია, სეგმენტში i-ურ სტრინგს მიენიჭება $x_i[0]$. იმ შემთხვევაში, თუკი შეტყობინების i-ური ბიტი 1-ია, მიენიჭება $x_i[1]$.

ხელმოწერის სიგრძეა n^2.

1.2.3 ხელმოწერის ვერიფიკაცია

ხელმოწერის ვერიფიკაციისთვის $sig = (sig_{n-1}, \ldots, sig_0)$, შეტყობინების ჰეში გამოითვლება.

$hash = (hash_{n-1}, \ldots, hash_0)$ და შემდეგი განტოლება უნდა შევამოწმოთ:

$(f(sig_{n-1}), \ldots, f(sig_0)) = (y_{n-1}[hash_{n-1}], \ldots, y_0[hash_0])$

თუ მართალია, ხელმოწერა სწორია.
ამ სქემის მთავარი და სერიოზული ნაკლი გასაღების დიდი ზომაა.

O (2^{80}) უსაფრთხოების მისაღწევად, ღია და დახურული გასაღებები უნდა იყოს 160∗2∗160 ბიტი = 51200 ბიტს, ეს 51200/1024=50-ჯერ დიდია, ვიდრე RSA-ს შემთხვევში.

ასევე უნდა ავღნიშნოთ, რომ მოცემულ სქემაში ხელმოწერის ზომა უფრო დიდია, ვიდრე RSA-ს შემთხვევაში. Winternitz-ის ერთჯერადი ხელმოწერის სქემა შემოთავაზებულია ხელმოწერის ზომის შესამცირებლად.

ერთჯერადი ხელმოწერის სქემები არაადეკვატურია უმეტესი პრაქტიკული სიტუაციებისთვის, რადგან გასაღების თითოეული წყვილის გამოყენება მხოლოდ ერთი ხელმოწერისთვისაა შესაძლებელი. 1979 წელს Ralph Merkle-მა შემოგვთავაზა ამ პრობლემის გადაწყვეტა. მისი იდეაა სრული ორობითი ჰეშის ხის გამოყენება. იდეა არის, რომ გამოვიყენოთ ბინარული ჰეშეპის ხე იმისათვის, რომ შევამციროთ ერთჯერადი ვერიფიკაციების გასაღებების რაოდენობა ერთი საჯარო გასაღებით, რომელიც იქნება ხის ფესვი.

2 Merkle-ს ხელმოწერის სქემა

ხის სიგრძე უნდა იყოს H>=2 და ერთი ღია გასაღებით 2^H, დოკუმენტზე ხელის მოწერა შეიძლება. ხელმოწერისა და ვერიფიკაციის 2^H წყვილი გენერირდება; X_i, Y_i, 0<=i<=2H. X_i არის ხელმოწერის გასაღები, Y_i კი ვერიფიკაციის.
ხეს ფოთლების გასაგებად, ხელმოწერის გასაღებების ჰეშირება შემდეგი ჰეშ ფუნქციის საშუალებით უნდა მოხდეს:

$$h:\{0,1\}^* \rightarrow \{0,1\}^n$$

მშობელი კვანძის მისაღებად, წინა ორი კვანძის კონკატენაციის ჰეშირება ხდება. ხის ფესვი ხელმოწერის ღია გასაღებია.

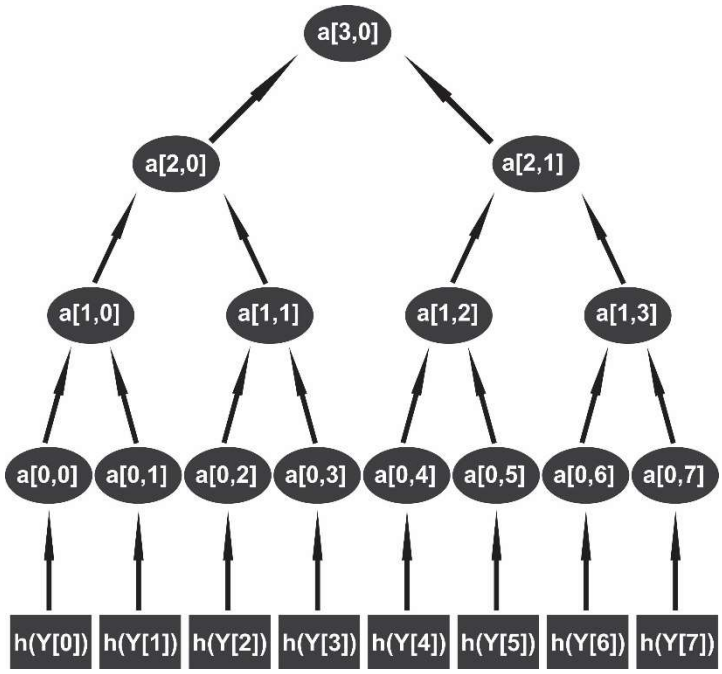

Fig. 1. Merkle-ს ხე, სადაც H=3

ფიგ.1 გამოსახულია ხე, სადაც H=3; a[i,j] კი ხის კვანძებია.

ნებისმიერი ზომის შეტყობინებაზე ხელმოწერისას, ჰეშირებით ზომა შეგვიძლია n-ის ტოლად გარდავქმნათ.
h (m) = hash, შეტყობინების ხელმოწერისთვის, გამოიყენება თვითნებური ერთჯერადი გასაღები X_{arb}. ხელმოწერა არის ერთობლიბა: ერთჯერადი ხელმოწერის, ერთჯერადი ვერიფიკაციის გასაღების, გასაღების ინდექსის და ყველა ძმა კვანძების, რომლებიც შერჩეულია თვითნებური გასაღებით, რომელთა ინდექსია "*arb*".

$$Signature = (sig||arb||\ Y_{arb}||auth_{0,\dots,}auth_{H-1}) \quad .$$

ხელმოწერის შემოწმებისთვის, ერთჯერადი ხელმოწერის კონტროლი შერჩეული ვერიფიკაციის გასაღებით ხდება. თუ ვერიფიკაცია გაიარა, ყველა საჭირო კვანძი გამოითვლება "auth"-ით, "arb" ინდექსითა და Y_{arb}. თუ ხის ფესვი ემთხვევა ღია გასაღებს, მაშინ ხელმოწერა სწორია.

ამ კრიპტოსისტემას ეფექტურობის პრობლემა აქვს, მისი გამოყენება პრაქტიკაში მიუღებელია [2-4].

ერთჯერადი გასაღებების 2^H წყვილი უნდა გამოვთვალოთ ღია გასაღების გენერირებისთვის. გასაღების ასეთი დიდი რიცხვის შენახვა პრაქტიკაში პრობლემურია.

3. Merkle ინტეგრირებული PRNG -ით

მსოფლიოს მეცნიერები მუშაობენ ამ სქემის გაუმჯობესებაზე. ერთ-ერთია PRNG-ს (ფსევდო შემთხვევითი რიცხვების გენერატორის) ინტეგრირება, რათა არ შევინახოთ გამოთვლები და დიდი ოდენობით ერთჯერადი გასაღების წყვილები [5,6].

ზოგიერთი PRNGs, რომლებიც ითვლებოდა უსაფრთხოდ შეგვიძლია კვანტური კომპიუტერით გავტეხოთ, ამიტომ ფრთხილად უნდა ვიყოთ PRNG-ის შერჩევისას.

Merkle-ში CSPRNG გვთავაზობს ჰეშ ფუნქციაზე დაფუძნებულ ალგორითმს, რადგან მასზე მთელი ალგორითმია დაფუძნებული. NIST-ის რეკომენდაციაა PRNGs-ზე დაფუძნებული ორი უწყვეტი ჰეში: HASH_DBRG და HMAC_DBRG. უკეთესია HASH_DBRG, რადგან უფრო ეფექტურია.

ჩვენ გთავაზობთ HASH_DBRG საწყისი მნიშვნელობების, თესლის, გენერაციისთვის ფიზიკური კვანტური შემთხვევითი რიცხვების (QRNG) გამოყენებას.

4. კვანტური შემთხვევითი რიცხვების გენერატორები

მე-20 საუკუნის მეორე ნახევარში კომპიუტერული სიმულაციის ზრდასთან ერთად, ელექტრონულ შემთხვევითი რიცხვების გენერატორებზე მოთხოვნაც გაიზარდა. იმ დროს, ჩვეულებრივი მოვლენა იყო შემთხვევითი რიცხვების ცხრილები. რადიოაქტიური დაშლა ხელმისაწვდომი წყაროა ჭეშმარიტი შემთხვევითობისთვის. Geiger-M¨uller-ის მილები მგრძნობიარეა α, β და γ რადიაციის აღმოჩენისა და გაძლიერებისთვის. მისი საშუალებით მივიღეთ საიმედო, კარგი რადიოაქტიული ნიმუშები. სიმარტივისთვის, რადიოაქტიურობაზე დაფუძნებული შემთხვევითი რიცხვების გენერატორები დაფუძნებული იყოს β რადიაციის აღმოჩენაზე.

Geiger-M¨uller, GM - ში ერთი ნაწილაკის დეტექტორი წარმოქმნის იონიზაციის მოვლენას, რომელიც Townsend avalanche-ში გაფართოვდება. შედეგად გვაქვს მოწყობილობა, რომელიც სწორად კონფიგურირების შემთხვევაში, თითოეული აღმოჩენილი ნაწილაკისთვის წარმოქმნის პულსს. ნებისმიერი ატომის დაშლის ალბათობა კონკრეტული დროის ინტერვალიში (t, t + dt) არის ექსპონენციალური შემთხვევითი ცვლადი, $P(t)dt = \lambda_m e^{\wedge}(-\lambda_m t)dt$, λ_m დაშლის მუდმივისთვის.

ეს QRNGs წარმოადგენს დღევანდელი ოპტიკური QRNG-ის წინამორბედს. გამოიყენება მსგავსი ცნებები და სქემები, მაგრამ რადიოაქტიური წყარო და GM მთვლელი, ფოტონის წყაროებითა და დეტექტორებითაა ჩანაცვლებული.

რადიოაქტიურ დაშლაზე დაფუძნებული პირველი კვანტური შემთხვევითი რიცხვების გენერატორები ბევრ საერთო ელემენტს იზიარებს. უმეტესობა იყენებს ციფრულ მთვლელს, დეტექტორიდან პულსების შემთხვევით ბიტებში კონვერტაციისთვის. ციფრული მრიცხველი ზრდის მის გამომავალ მნიშვნელობას 1-ით, როდესაც მნიშვნელობად მიიღებს პულსს და შეუძლია გადატვირთოს - დაიწყოს თვლა ნულიდან. კიდევ ერთი მნიშვნელოვანი ელემენტია ციფრულ საათთან სინქრონიზაცია. ამ QRNGs უკეთესად განვმარტავთ თუ აღვწერთ საათებს, სწრაფი და ნელი საათის ტერმინით, ν სიხშირით, რომელიც აღმოჩენის საშუალო მაჩვენებელს მნიშვნელოვნად აღემატება ან გაცილებით მცირეა. სწრაფი საათი, სადაც $\nu > \lambda$, აგენერირებს ბევრ პულსს, Geiger-ის მთვლელებს შორის. ნელ საათში, სადაც $\nu < \lambda$, უნდა იყოს გასული საკმარისი დრო, GM დეტექტორმა უნდა დაარეგისტრიროს საკმარისი ოდენობის პულსები.

ამ ელემენტებით, აღმოჩენის დროის შემთხვევითობა შეიძლება გარდავქმნათ რამდენიმე გზით შემთხვევით ციფრებში. გენერატორები Isida და Ikeda, ასევე Vincent იყენებს სწრაფ საათიან მრიცხველს, სადაც ყოველი აღმოჩენილი მნიშვნელობა იკითხება და შემდეგ ნულდება (ყოველ ჯერზე, როცა დეტექტორზე მნიშვნელობას ვიღებთ). აღმოჩენის მომენტში მრიცხველის მნიშვნელობა გამოიყენება შემთხვევითი რიცხვის წარმოსაქმნელად. მნიშვნელობების განაწილება არ არის თანაბარი, საჭიროებს შესწორებას. თუ წარმოვქმნით ათობით ციფრს, შეგვიძლია ავიღოთ ყველაზე ნაკლებად მნიშვნელოვანი ფიგურა. ოროობითი მიმდევრობისთვის ექვივალენტური მეთოდია მრიცხველის მნიშვნელობის ტოლობის შემოწმება, დათვლილი პულსების მნიშვნელობა კენტია თუ ლუწი.

მეორე ვარიანტია, ნელი საათის გამოყენება, რათა დავადგინოთ როდის წავიკითხოთ მრიცხველი. Schmidt-ის გენერატორში GM-ის დეტექტორის პულსები მრიცხველის მნიშვნელობას ზრდის. როდესაც ნელი საათი წარმოქმნის ახალ პულსს, მრიცხველის მნიშვნელობა გამოიყენება, როგორც შემთხვევითი ციფრი და ათვლა კვლავ იწყება 0-დან. გამომავალი მნიშვნელობა შეესაბამება თითოეული საათის პერიოდში ნაწილაკების ოდენობას. ჩვენ ვზღუდავთ მრიცხველს, რომელიც აგენერირებს 0 დან M−1-მდე მნიშვნელობებს. ეს არის მოდულით M მრიცხველი. როდესაც M = 2, გვაქვს ოროობითი შემთხვევითი რიცხვების გენერატორი. შერჩეული ციფრების განაწილება არ არის თანაბარი, მაგრამ თუ ავიღებთ M მოდულით და მრავალჯერ გამოვიტანთ მნიშვნელობებს, მივიღებთ მიკერძოებას სასურველად მცირე განაწილებით. ამ პროცესს ეწოდება "შეკუმშვა ". რადიოაქტიური დაშლა ასევე გამოიყენება ანალოგური კომპიუტერებისთვის თეთრი ხმაურის შესაქმნელად. შემთხვევითი ხმაურის გენერატორებს მნიშვნელოვანი როლი ჰქონდათ თვითმფრინავის დიზაინის სიმულაციაში, ანალოგურ გამოთვლებში. ის ასევე გამოიყენება, როგორც სატესტო სიგნალი, ზოგადად ისეთ კომუნიკაციისა და სიმულაციის პრობლემებში სადაც მაღალგამტარი სიგნალია საჭირო. ამ შემთხვევაში, GM გამტარიდან პულსები იწვევს ძაბვის სიგნალის შეცვლას. როდესაც ნაწილაკი გამოვლინდება, სიგნალი მაღალიდან დაბალი ძაბვიდან გადადის დაბალიდან მაღალში. შედეგად მიღებულ შემთხვევით სიგნალს შემთხვევით ტელეგრაფიულ ხმაურს უწოდებენ. ამ დროს არ გვინდა ოროობითი სიგნალი, არამედ Gaussian-ის ხმაური.

5. გამოწვევები

მიუხედავად იმისა, რომ რადიოაქტიურ დაშლაზე დაფუძნებული QRNGs გვაძლევს კარგი ხარისხის ჭეშმარიტ შემთხვევით რიცხვებს, აქვთ ნაკლოვანებები, რომლებიც ზღუდავს მათ პრაქტიკულ გამოყენებას. მნიშვნელოვანი ბარიერია ბიტების სიჩქარე, ჩვეულებრივ, რამდენიმე ასეული კილობიტი წამში.

პირველი პრობლემა რადიოაქტიური წყაროს საჭიროებაა. პრინციპში, ყველა დაშლაზე დაფუძნებული QRNGs მუშაობს ფონურ რადიაციაზე. თუ დეტექტორი იზილირებული არ არის, შეუძლია დაითვალოს მოხეტიალე კოსმოსური სხივები, რადიაცია რადიუმიდან, თორიუმიდან და სხვა რადიოაქტიური მასალებიდან, რომლებიც დედამიწის ქერქში ან ჰაერშია. თუმცა, ბუნებრივი იშვიათად წარმოქმნის საჭირო ნაწილაკებს, რომლებიც ერთ წამში რამდენიმეზე მეტი იქნება. ეს არის ფუნდამენტური პრობლემა, რომელიც რადიოაქტიური დაშლის QRNGs ფართოდ გამოყენებას ხელს უშლის. სწრაფი ტემპის მისაღწევად, QRNG-ს სჭირდება ძალიან რადიოაქტიური წყარო. მაგალითად გენერატორები იყენებენ Cobalt-60, Strontium-90, Caesium-137, Americium-241 ან Nickel-63. ეს მოუხერხებელია და მოითხოვს უსაფრთხოების გაუმჯობესებას. მიუხედავად იმისა, რომ α წყარო, როგორიცაა Americium ადვილად იზოლირებადია და გავრცელებულია კვამლის სიგნალებში, დამატებითი სიფრთხილის ზომები ხელს უშლის კომპიუტერთან ინტეგრაციას. ეს მიდგომა კარგად მუშაობს მხოლოდ ისეთ სპეციალურ სერვერებთან, როგორიცაა HotBits.

გენერირებული ბიტების სისწრაფის მეორე შეზღუდვაა დეტექტორების მკვდარი დრო. Geiger-ის მთვლელში avalanche, რომელიც ზრდის თითოეულ დათვლას, GM მილში ხდება გაზის იონიზაცია. avalanche ჩერდება, როდესაც დადებითი იონები შემოერტყმება cathode მილში. ეს იონები გვიცავს უფრო მეტი avalanche-დან, სანამ ნორმალურ მდგომარეობაში დაბრუნდებიან. მკვდარი დრო არის, GM მილის მინიმალური დრო, რომელიც საჭიროა სრულ აღმოჩენის უნარის დაბრუნებამდე. ეს დრო შეიძლება იყოს ათეულობით ნანოწამიდან რამდენიმე მიკროწამამდე. ეს ზღუდავს დათვლის სიჩქარეს MHz დიაპაზონში. ნახევრადგამტარ გამტარებს ასევე სჭირდებათ მკვდარი დრო თითოეული აღმოჩენის შემდეგ, რომელიც მიკროწამის დიაპაზონშია.

მკვდარ დროს და სხვა არაერთგვაროვან წყაროებს სჭირდებათ დამუშავება, როდესაც შემთხვევითი ბიტების გენერაცია ხდება. ზოგადად, დაგენერირებული ბიტების ხარისხი კარგი იქნება და როდესაც არის დარჩენილი რაღაც მიკერძოება, არსებობს მარტივი დამუშავების მეთოდები, რომლებიც აღადგენენ შემთხვევით მიღებულ მნიშვნელობებს.

საბოლოო პრობლემა ნახევარგამტარ დეტექტორებს ეხება. მათზე მოქმედებს რადიაცია. Geiger მილებიც დროთა განმავლობაში იცვითება, მაგრამ მათზე რადიაციის ეფექტი უკვე შესწავლილია, ხოლო კონკრეტულად რადიაციის დეტექტორებისთვის ნახევარგამტარები ახალია. საჭიროა ამ საკითხის დროის განმავლობაში შესწავლა.

ამ შეზღუდვების მიუხედავად, რადიოაქტიური დაშლა შემთხვევითობის შესაფერისი წყაროა, დაბალი სიჩქარის მოწყობილობებისთვის. მაგალითად, მას შეუძლია მოგვაწოდოს ენტროფია ფსევდო შემთხვევითი რიცხვების გენერატორების საწყისი მნიშვნელობებისთვის. უფრო

მომთხოვნი სისტემებისთვის, რომლებიც ბიტების მაღალ სიხშირეს მოითხოვენ ან როცა გვინდა თავი ავარიდოთ რადიოაქტიურ წყაროებს, უახლესი QRNGs კარგი ჩანაცვლებაა.

6. სქემა

ხის ზომა უნდა იყოს H>=2 და დოკუმენტზე ხელმოწერა შეიძლებოდეს ერთი 2^H ღია გასაღებით. კვანტური შემთხვევითი რიცხვების გენერატორებით წარმოვქმნით საწყის მნიშვენლობებს. PRNG HASH_DBRG იღებს ამ საწყის მნიშვნელობას, როგორც შემავალ მნიშვნელობად და აგენერირებს ხელმოწერისა და ვერიფიკაციის გასაღებებს; X_i, Y_i, 0<=i<=2H. X_i არის ხელმოწერის გასაღები, Y_i - ვერიფიკაციის გასაღები. ხეზე ფოთლების მისაღებად, ჰეშ ფუნქციით ხელმოწერის გასაღებების ჰეშირება ხდება:

$$h:\{0,1\}^* \rightarrow \{0,1\}^n \quad .$$

მშობელი კვანძის გასაგებად, წინა ორი კვანძის კონკატენაციის ჰეშირებაა საჭირო. ხის ფესვი არის ხელმოწერის ღია გასაღები.

ნებისმიერი ზომის შეტყობინებაზე ხელმოწერისას, ჰეშირებით ზომა შეგვიძლია n-ის ტოლად გარდავქმნათ.

h (m) = hash, შეტყობინების ხელმოწერისთვის, გამოიყენება თვითნებური ერთჯერადი გასაღები X_{arb}. ხელმოწერა არის ერთობლიბა: ერთჯერადი ხელმოწერის, ერთჯერადი ვერიფიკაციის გასაღების, გასაღების ინდექსის და ყველა ძმა კვანძების, რომლებიც შერჩეულია თვითნებური გასაღებით, რომელთა ინდექსია "*arb*".

$$Signature= (sig||arb|| Y_{arb}||auth_0,\ldots,auth_{H-1})$$

ხელმოწერის შემოწმებისთვის, ერთჯერადი ხელმოწერის კონტროლი შერჩეული ვერიფიკაციის გასაღებით ხდება. თუ ვერიფიკაცია გაიარა, ყველა საჭირო კვანძი გამოითვლება "auth"-ით, "arb" ინდექსითა და Y_{arb}. თუ ხის ფესვი ემთხვევა ღია გასაღებს, მაშინ ხელმოწერა სწორია.

7. დასკვნა

მიღებული სქემა საკმაოდ ეფექტურია, რადგან არ ინახავს ხელმოწერის ყველა გასაღებს. იყენებს კვანტურად მდგრად ფსევდო შემთხვევითი რიცხვების გენერატორს, რომელიც იყენებს ჰეშ ფუნქციებს და არის NIST სტანდარტი. ის გენერატორი საწყის მნიშვნელობებს იღებს კვანტური შემთხვევითი რიცხვების გენერატორიდან. გაანალიზებულია კვანტური შემთხვევითი რიცხვების გენერატორების გამოყენების გამოწვევები.

ACKNOWLEDGEMENT

The work was conducted as a part of PHDF-19-519 and the grant financed by Caucasus University

ბიბლიოგრაფია

1. Ajtai, M.: Generating hard instances of lattice problems. In Complexity of computations and proofs, volume 13 of Quad. Mat., pages 1–32. Dept. Math., Seconda Univ. Napoli, Caserta (2004). Preliminary version in STOC 1996. 8. Babai, L.: On Lovász lattice reduction and the nearest lattice point problem. Combinatorica, 6:1–13 (1986).
2. A Gagnidze, M Iavich, G Iashvili, Novel Version of Merkle Cryptosystem - Bull. Georg. Natl. Acad. Sci, 2017
3. Buldas A., Firsov D., Laanoja R., Lakk H., Truu A. (2019) A New Approach to Constructing Digital Signature Schemes. In: Attrapadung N., Yagi T. (eds) Advances in Information and Computer Security. IWSEC 2019. Lecture Notes in Computer Science, vol 11689. Springer, Cham
4. Post-quantum cryptosystems // Modern scientific researches and innovations. 2016. № 5 [Electronic journal]. URL: http://web.snauka.ru/en/issues/2016/05/67264
5. A.Gagnidze, M.Iavich, G. Iashvili, MERKLE WITH QUANTUM TRNG, Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):14-20, 2017
6. Buchmann J., García L.C.C., Dahmen E., Döring M., Klintsevich E. (2006) CMSS – An Improved Merkle Signature Scheme. In: Barua R., Lange T. (eds) Progress in Cryptology - INDOCRYPT 2006. INDOCRYPT 2006. Lecture Notes in Computer Science, vol 4329. Springer, Berlin, Heidelberg