Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 1 – 13 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ახალი პოსტკვანტური ციფრული ხელმოწერა ვერკლის ხისა და ლატისების გამოყენებით

NOVEL POST-QUANTUM DIGITAL SIGNATURE USING VERKLE TREES AND LATTICES

Maksim Iavich[1], Tamari Kuchukhidze[2], Avtandil Gagnidze[3]

[1] Department of Computer Science, Caucasus University, 0102, Georgia
[2] Department of Computer Science, Caucasus University, 0102, Georgia
[3] East West University, Tbilisi, Georgia

რეზიუმე: ბოლო წლებში კვანტურ კომპიუტერებზე კვლევები მნიშვნელოვნად განვითარდა. თუ კაცობრიობა ოდესმე შექმნის ეფექტურ კვანტურ კომპიუტერს, არსებული საჯარო გასაღების უმეტესი კრიპტოსისტემა შეიძლება დაზარალდეს. ეს კრიპტოსისტემები დღსდღეობით გვხვდება ბევრ კომერციულ პროდუქტში. ჩვენ შევიმუშავეთ შედეგები, რომლებიც, როგორც ჩანს გვიცავს კვანტური შეტევებისგან, მაგრამ ისინი სახიფათო და არაეფექტურია ყოველდღიურ ცხოვრებაში გამოსაყენებლად. ნაშრომში გაანალიზებულია ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის მეთოდები. შეფასებულია მერკლის ხეზე დაფუძნებული ელექტრონული ხელმოწერა. ვერკლის ხის და ვექტორული ვალდებულებების გამოყენებით ნაშრომი იკვლევს ახალ იდეებს.
ამ სტატიაში წარმოვადგენთ უნიკალურ ტექნოლოგიას, პოსტკვანტური ციფრული ხელმოწერის სისტემის შემუშავებისთვის ვიყენებთ უახლეს ვერკლის ხეს. ამ მიზნისთვის გამოიყენება ვერკლის ხე, ვექტორული ვალდებულებები და ისეთი ვექტორული ვალდებულებები, რომლებიც დაფუძნებულია ლატისებზე, პოსტკვანტური თვისებებისთვის. ნაშრომში ასევე მოცემული პოსტკვანტური ხელმოწერის დიზაინის ცნებები ვერკლის ხის გამოყენებით.

საკვანძო სიტყვები: კვანტური კრიპტოგრაფია, ვექტორული ვალდებულებები, ლატისებზე დაფუძნებული ვექტორული ვალდებულებები, ვერკლის ხე, კრიპტოგრაფიული გამოყენება.

ABSTRACT: Research on quantum computers has advanced significantly in recent years. If humanity ever creates an effective quantum computer, many of the present public key cryptosystems can be compromised. These cryptosystems are currently found in many commercial products. We have devised solutions that seem to protect us from quantum attacks, but they are unsafe and inefficient for use in everyday life. In the paper, hash-based digital signature techniques are analyzed. Merkle tree based digital signature is assessed. Using a Verkle tree and vector commitments, the paper explores the novel ideas.
The authors of this article present a unique technology for developing a post-quantum digital signature system using state-of-the-art Verkle tree technology. Verkle tree, vector commitments, and vector commitments based on lattices for post-quantum features are used

for this purpose. The concepts of post-quantum signature design utilizing Verkle Tree are also provided in the paper.

Keywords: quantum cryptography; vector commitments; lattice-based vector commitments; Verkle tree; cryptographical application.

1. შესავალი

მოსალოდნელია, რომ კვანტური გამოთვლები მომავალში უფრო გავრცელდება, რაც გამოიწვევს პოსტკვანტური კრიპტოგრაფიის განვითარებას, ტექნიკას, რომელიც იცავს კვანტური კომპიუტერების თავდასხმებისგან. კვანტურ კომპიუტერებს შეუძლიათ უფრო სწრაფად შეასრულონ რთული გამოთვლები, ვიდრე ჩვეულებრივი კომპიუტერები. კვანტური კომპიუტერი ასრულებს დავალებებს რამდენიმე წამში, ხოლო კლასიკურ კომპიუტერს რამდენიმე წელი სჭირდება. კვანტურმა კომპიუტერმა შეიძლება დაარღვიოს სტანდარტული კრიპტო სისტემების უმეტესობა, თუ არა ყველა, რომელიც ამჟამად ვიყენებთ პრაქტიკაში [1-2].

RSA-ზე დაფუძნებული სისტემებს, რომლებსაც ფართოდ ვიყენებთ კომერციულ პროდუქტებსა და აპლიკაციებში, ემუქრებათ გატეხვა პოსტკვანტურ კრიპტოსისტემებში. RSA სისტემების ალტერნატივები, როგორიცაა ჰეშირებაზე დაფუძნებული ხელმოწერის სქემები, შემოთავაზებულია, მაგრამ არ არის პრაქტიკული უსაფრთხოების ან ეფექტურობის გამო. ამ სისტემების უსაფრთხოება დამოკიდებულია ჰეშირების ფუნქციის უნარზე, წინააღმდეგობა გაუწიოს შეჯახებებს ანუ კოლიზიებს [3].

უსაფრთხო პოსტკვანტური კრიპტოსისტემების შემუშავება და დანერგვა შრომატევადი პროცესია. როგორც კი კვანტური გამოთვლები გავრცელდება, RSA და სხვა ასიმეტრიული ალგორითმები ვეღარ შეძლებენ პირადი მონაცემების დაცვას. მიზანია შექმნას RSA კრიპტოსისტემის შემცვლელები, რომლებსაც გაუძლებენ კვანტური კომპიუტერის შეტევებს, როგორიცაა ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემები, რომლებიც უსაფრთხოა კრიპტოგრაფიული ჰეშირების ფუნქციების გამო [4].

ნაშრომში განხილულია ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის სქემები მერკლის ხეების გამოყენებით, რომლებიც პოსტკვანტურია და შეუძლიათ წინააღმდეგობა გაუწიონ კვანტურ შეტევებს. თუმცა, ამ სქემებს აქვთ დიდი ხელმოწერის ზომები. NIST-მა მიიღო ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერა SPHINC+, მაგრამ მას მაინც აქვს ეფექტურობის პრობლემები. ვერკლის ხეები, მერკლის ხეების განახლებული ვარიანტი გვთავაზობს უფრო ეფექტურ ვერიფიკაციის პროცედურებს, მხოლოდ არსებითი ინფორმაციის შენარჩუნებით. ეს ამცირებს შესანახ ადგილს ლოკალურ სივრცეში და შეუძლია მნიშვნელოვნად შეამციროს ხელმოწერის ზომა.

ნაშრომში წარმოდგენილია ახალი პოსტკვანტური ციფრული ხელმოწერის მოდელი, რომელიც იყენებს ვერკლის ხეებს. მოდელი დაფუძნებულია პოსტკვანტური თვისებების მქონე ლატისებზე დამყარებული ვექტორული ვალდებულებების გათვალისწინებით.

2. ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის სქემები

ჰეშირებაზე დაფუძნებული ხელმოწერის სქემები არის კრიპტოგრაფიული მეთოდები, რომლებიც ქმნის ციფრულ ხელმოწერებს კრიპტოგრაფიული ჰეშირების ფუნქციების გამოყენებით. ამ სქემებს აქვთ უპირატესობა, რომ არ ეყრდნობიან მათემატიკურ სირთულეებს, როგორიცაა დიდი რიცხვების ფაქტორიზაცია ან ელიფსური მრუდის დისკრეტული ლოგარითმების ამოხსნა, შედეგად მათი გამოყენება შესაძლებელია პოსტკვანტურ ეპოქაში. NIST-მა აირჩია სამი ალგორითმი ციფრული ხელმოწერებისთვის, მათ შორის CRYSTALS-Dilithium, FALCON და SPHINCS+.

ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის მეთოდები მოიცავს გასაღების შექმნას, ხელმოწერის შექმნას და ხელმოწერის ვერიფიკაციას/გადამოწმებას. პირადი გასაღები წარმოიქმნება საიდუმლო გასაღების შემთხვევითი გენერირებით, რომელიც აუცილებლად დაცული უნდა იყოს. შემდეგ, კონკრეტული კომუნიკაციისთვის ხელმოწერის შესაქმნელად, შეტყობინებაზე ვმოქმედეთ საიდუმლო გასაღების და ჰეშის ფუნქციის განმეორებით გამოყენებით. მიმღები ადასტურებს ხელმოწერის ლეგიტიმურობას მესიჯის საჯარო გასაღებთან კონკატენაციით.

ჰეშირებაზე დაფუძნებულ ერთჯერადი ხელმოწერის მეთოდებს დიდი პოტენციალი გააჩნიათპოსტკვანტური ეპოქისთვის. განსაკუთრებით ისეთ სქემებს, რომლებიც ეყრდნობა კრიპტოგრაფიული ჰეშის ფუნქციების კოლიზიის მიმართ წინააღმდეგობას. ამის მაგალითია Lamport-Diffie ერთჯერადი ხელმოწერის (LDOTS) სქემა [6-7].

Lamport-Diffie ერთჯერადი ხელმოწერები იქმნება ცალმხრივი ფუნქციისა და კრიპტოგრაფიული ჰეშრების ფუნქციის გამოყენებით. გასაღების წყვილი გენერირდება n სიგრძის 2n ბიტის შემთხვევითი სტრიქონის გამოყენებით. LDOTS ხელმოწერის გასაღები X, არჩეულია შემთხვევით:

$$X = (x_{n-1}[0], x_{n-1}[1], \dots, x_1[0], x_1[1], x_0[0], x_0[1]) \epsilon R \{0,1\}^{(n,2n)} \quad (1)$$

Lamport-Diffie ერთჯერადი ხელმოწერის ვერიფიკაციის გასაღები არის Y, რომელიც გამოითვლება ფორმულა (2)–ის საშუალებით:

$$Y = (y_{n-1}[0], y_{n-1}[1], \dots, y_1[0], y_1[1], y_0[0], y_0[1]) \epsilon \{0,1\}^{(n,2n)} \quad (2)$$

გასაღების გამოთვლა ხორციელდება ცალმხრივი ფუნქციის f–ის გამოყენებით, როგორც ეს აღწერილია (3) ფორმულით:

$$y_i[j] = f(\ x_i[j]), 0 \le i \le n-1, j = 0,1. \quad (3)$$

ამიტომ, Lamport-Diffie-ის ერთჯერადი ხელმოწერის გასაღების გენერაცია მოითხოვს f-ის 2n შეფასებას. n სიგრძის 2n-ბიტიანი სტრიქონები ქმნიან ხელმოწერისა და ვერიფიკაციის გასაღებებს. თუ LDOTS ხელმოწერა გენერირებულია, დოკუმენტი $M \epsilon \{0,1\}^*$ ხელმოწერილია

LDOTS–ის გამოყენებით, X ხელმოწერის გასაღებით. M-ის შეტყობინების დაიჯესტი არის is $g(M) = d = (d_{n-1}, \dots, d_0)$. LDOTS ხელმოწერა არის $sign = (x_{n-1}[d_{n-1}], \dots, x_1[d_1], x_0[d_0]) \epsilon \{0,1\}^{(n,n)}$.

ამ ხელმოწერის ასაგებად გამოიყენება n ბიტიანი სტრიქონების სიგრძე. ეს სტრიქონები ირჩევა, როგორც d ფუნქცია შეტყობინებების შეჯამებისთვის/დაიჯესტისთვის. ჩვეულებრივი იმის გასაზომვა, თუ რამდენი კრიპტოგრაფიული ოპერაციების შესრულება შეუძლია CPU-ს ერთდროულად, არის ჰეშებზე დაკვირვება წამში [8].

Winternitz-ის ერთჯერადი ხელმოწერის სქემა (WOTS) რეკომენდებულია ხელმოწერების რაოდენობის შესამცირებლად. ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის სტრუქტურები უზრუნველყოფს საიდუმლო გასაღების გამოყენებას მხოლოდ ერთხელ, ერთი ხელმოწერის შესაქმნელად, რაც საშუალებას გვაძლევს ელექტრონული ხელმოწერების სიზუსტეს და ლეგიტიმურობას. რეალური სამყაროში, ერთჯერადი ხელმოწერის მიდგომები არაეფექტურია, ამიტომ რალფ მერკლი გვირჩევს გამოიყენოს სრული ორობითი ჰეშირების ხე, რომ შევზღუდოთ ერთჯერადი ვერიფიკაციის გასაღებების თვითნებური რაოდენობის ავთენტურობა ერთი საჯარო გასაღებით.

3. მერკლის ხის ავთენტიფიკაციის სქემა

მერკლის ხის საშუალებით შეგვიძლია გადავწყვიტოთ მრავალრიცხოვანი დაიჯესტის (n) შენახვის პრობლემა ერთჯერადი ხელმოწერის სქემებისთვის, რადგან თითოეული შეტყობინება მოითხოვს სხვადასხვა გასაღების წყვილს. ეს სისტემა იყენებს ბინარულ ხის სტრუქტურას და კრიპტოგრაფიულ ჰეშირების ფუნქციას უსაფრთხო და სანდო ხელმოწერების შესაქმნელად. მერკლის იყენებს კრიპტოგრაფიულ ჰეშირების ფუნქციას g, $g : \{0,1\}^* \rightarrow \{0,1\}^n$ ნებისმიერი სიგრძის ორობითი სტრიქონს გადაიყვანს, n ფიქსირებული სიგრძის ორობით სტრიქონად. როდესაც ხელმომწერი ირჩევს $H \in \mathbb{N}$, სადაც $H \geq 2$, ქმნის მერკლის ხელმოწერის სქემის (MSS) გასაღებების წყვილს. შესაბამისად, იქმნება გასაღების წყვილი. ეს საშულებას გვაძლევს ხელი მოვაწეროთ და დავამოწმოთ 2^H დოკუმენტი. უნდა აღინიშნოს, რომ ეს მნიშვნელოვნად განსხვავდება ხელმოწერის პროტოკოლებისგან, როგორიცაა RSA და ECDSA, სადაც ერთი გასაღების წყვილი შეიძლება გამოვიყენოთ დიდი რაოდენობის დოკუმენტების ხელმოწერისთვის/დამოწმებისთვის. მიუხედავად ამისა, პრაქტიკაში, ეს მაჩვენებელი ასევე შეზღუდულია ხელმოწერის შესაქმნელად გამოყენებული ინსტრუმენტებით ან კონკრეტული შეზღუდვებით [9].

მერკლის ხე აგენერირებს გასაღების წყვილს თითოეული $0 \leq j < 2^H$ – თვის, რაც იძლევა 2^H დოკუმენტების ხელმოწერისა და ვალიდაციის საშუალებას. მერკლის ხის შიდა კვანძები განისაზღვრება ფორმულით, რომელიც უდრის მისი მარცხენა და მარჯვენა შვილების ჯამს. მერკლის ხის საფუძველი არის მერკლის ხელმოწერის სქემის (MSS) საჯარო გასაღები. 2^H ხელმოწერის გასაღებების სერია ქმნის MSS საიდუმლო გასაღებს [10].

მერკლის ხე წარმატებით იყენებს ერთჯერადი ხელმოწერის გასაღებებს ხელმოწერების გენერირებისთვის. ხელმომწერი ითვლის n-ბიტ $d = g(M)$, რისი საშუალებით ხელს აწერს

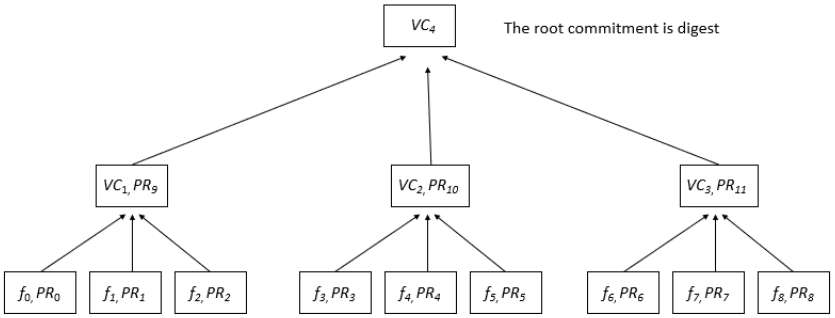
შეტყობინებას. შემდეგ ქმნის ერთჯერად ხელმოწერას $sign_{OTS}$, იყენებს s-ურ ერთჯერადი ხელმოწერის გასაღებს $X_s, s \in \{0, \dots, 2^H - 1\}$. რომ დავადასტუროთ Y_s, ხელმომწერი ამატებს ავთენტიფიკაციის გზას და ინდექს s–ს, ვერიფიკაციის გასაღებ Y_s –ს.

მერკლის ხეები გამოთვლა სწრაფად შეგვიძლია და მისი შექმნა შესაძლებელია O(n) დროში. თუმცა, ხის სიმაღლე უნდა იყოს n, თუ გვსურს ხელი მოვაწეროთ 2^n შეტყობინებას. ასევე, მერკლის მტკიცებულების ლოკალურად შენახვა არ არის პრაქტიკული და რთულია.

4. ვერკლის ხე

ვერკლის ხე მერკლის ხის მსგავსი სტრუქტურაა, რომელიც ეფექტურობით, მოქნილობითა და მასშტაბურობის თვალსაზრისით აღემატება მერკლის ხეს. ვერკლის ხის საშუალებით გვაქვს უფრო მცირე ვერიფიკაცია და უფრო ეფექტურია, ვიდრე მერკლის ხეები, რომლებიც მოითხოვს მეტ დამუშავებას და შესანახ ტევადობას, კრიპტოგრაფიული მონაცემების ზრდის გამო. ვერკლის ხე ამცირებს ზედმეტ მონაცემების დამუშავებას, რაც გამოწვეულია შუალედური კვანძების შენახვით. ის ამცირებენ შემოწმებისთვის საჭირო ჰეშის გამოთვლების რაოდენობას. ასევე აქვთ მასშტაბურობა, რაც შესაფერისს ხდის მასიური მონაცემთა ბაზების ეფექტურად მართვისთვის. შესაბამისად, ვერკლის ხე უფრო ეფექტულია შეზღუდული რესურსების მქონე აპლიკაციებისთვის [11].

ვერკლის ხის პირველადი მტკიცება არის ის, რომ ვექტორული ვალდებულებები შეიძლება გამოვიყენოთ კრიპტოგრაფიული ჰეშირების ფუნქციების ნაცვლად, რომელიც საჭიროა მერკლის ხის შესაქმნელად. ეს გულისხმობს ავირჩიოთ რაოდენობა რამდენ ნაწილად დაიყოფა ხე (k ნაწილი და ვექტორული ვალდებულება გამოვთვალოთ თითოეულ ნაწილზე. ვერკლის ხე საჭიროებს განსხვავებულ მიდგომას მტკიცებულების მიწოდების კუთხით, ეყრდნობა batching კვანძებს", რომელიც ამოწმებს რამდენიმე გზას ერთდროულად, რაც მნიშვნელოვნად ამცირებს ინფორმაციას, რაც საჭიროა მტკიცებულებების დასადგენად [12].



ფიგურა 1. ვერკლის ხე - $K = 3$

ვერკლის ხეებს არ სჭირდებად დედმამიშვილი კვანძებიც კი, განსხვავებით მერკლის ხისგან. ვერკლის ხეს დამტკიცებისთვის მხოლოდ გზა და მცირეოდენი დამატებითი ინფორმაცია სჭირდება.

ვერკლის ხე ითვლის შიდა კვანძს მისი შთამომავლისგან, ჰეშირების ალგორითმის გამოყენებით, რომელიც განსხვავდება ჩვეულებრივი ჰეშისგან. ამის ნაცვლად გამოიყენება ვექტორული ვალდებულება. ვერკლის ხის პირველადი განცხადება არის ის, რომ მერკლის ხე შეიძლება შეიქმნას თუკი კრიპტოგრაფიულ ჰეშირების ფუნქციას ჩავანაცვლებთ ვექტორული ვალდებულებებით. ვერკლის ხის საშუალებით შეგვიძლია მივაღწიოთ იგივე მიზანს, როგორც მერკლის ხის გამოყენებთ. მთავარი განსხვავება არის ის, რომ ახალი ვერკლის ხე ბევრად უფრო ეფექტურია.

5. ვექტორული ვალდებულება

ვალდებულების სქემები არის კრიპტოგრაფიული საფუძვლის მნიშვნელოვანი ნაწილი, რომლებიც საშუალებას გვაძლევს დავმალოთ მნიშვნელობა და მოგვიანებით გამოვაჩინოთ დამალული მნიშვნელობა. ვალდებულებების სისტემების ორი არსებითი მახასიათებელია დამალვა, რომელიც ავლენს მნიშვნელობას საჭიროების შემთხვევაში და შებოჭვა (binding), რომელიც ზღუდავს წვდომას სხვა მნიშვნელობებზე. ვექტორული ვალდებულებების (VC) სქემები აფართოებს ამ მახასიათებლებს მნიშვნელობების თანმიმდევრობების და პოტენციური ატრიბუტების დამალვის საშუალებით. ეს ართულებს ერთდროულად სხვადასხვა მნიშვნელობების გახსნას [13].

ვექტორული ვალდებულებები (Vector commitments) საჭიროა პოზიციის შებოჭისთვის, რადგან მოწინააღმდეგეს არ უნდა შეეძლოს ერთდროულად ორ სხვადასხვა მნიშვნელობის ღიად აღება (commit). ვალდებულების სტრიქონის სიგრძე და თითოეული გახსნის ზომა დამოუკიდებელი უნდა იყოს ვექტორის სიგრძისგან, რათა დააკმაყოფილოს კრიტერიუმები. ვექტორულ ვალდებულებებს შეიძლება ასევე დასჭირდეს უსაფრთხოების თვისება, როგორიცაა დამალვა, რომელიც ითვალისწინებს, რომ ძნელი უნდა იყოს დადგენა, იყო თუ არა ვალდებულება ვექტორიდან $(m_1, \dots, m_q)$, ან თუ ვექტორიდან $(m'_1, \dots, m'_q)$ [14].

გვაქვს შემდეგი ალგორითმები ვექტორული ვალდებულებებისთვის:

$\mathrm{Setup}(1^{\gamma}, 1^{\mathrm{d}})$ - ალგორითმი იღებს უსაფრთხოების პარამეტრს γ და მნიშვნელობა d–ს, როგორც შემომავალ მნიშვნელობას და აგენერირებს საჯარო კომიტერის (committer) პარამეტრებს cp და ვერიფიკატორის პარამეტრებს vp.

$\mathrm{Commit}(\mathrm{cp}, \mathrm{m} \in \mathrm{M}^{\mathrm{d}})$ - Committer პარამეტრების cp და შეტყობინების m, რომელიც მოცემულია M^{d} სივრციდან, გათვალისწინებით, ეს ალგორითმი გვაძლევს ვალდებულებას $\mathrm{c} \in \mathrm{Com}$ და კომიტერის მდგომარეობას st.

$\mathrm{Open}(\mathrm{cp}, \mathrm{st}, \mathrm{i} \in [\mathrm{d}])$ - კომიტერის პარამეტრების cp, კომიტერის მდგომარეობის st და i ინდექსის გათვალისწინებით d დიაპაზონიდან, ეს ალგორითმი გვაძლევს მტკიცებულებას pr_i–სშეტყობინების i-ურ ჩანაწერისთვის st.

$\mathrm{Verify}(\mathrm{vp}, \mathrm{c} \in \mathrm{Com}, \mathrm{i} \in [\mathrm{d}], \mathrm{m} \in \mathrm{M}, \mathrm{pr} \in \mathrm{Pr})$ – ეს ალგორითმი იღებს დამადასტურებელ პარამეტრებს vp, ვალდებულება c, ინდექსი i, შეტყობინება m და მტკიცებულება pr შემავალი მნიშვნელობების სახით და განსაზღვრავს თუ არა მტკიცებულება რეალური არის თუ არა.

თუ სქემა აკმაყოფილებს ზემოხსენებულ ინტერფეისებს, ის იძლევა მოდიფიკაციების განხორციელების საშუალებას committed შეტყობინების ვექტორში შესაბამისი ვალდებულების, მტკიცებულების და მდგომარეობის განახლებებით.

განახლების სქემის სისწორის პირობა იძლევა გარანტიას, რომ ორი ექსპერიმენტის შედეგი სტატისტიკურად იდენტურია ნებისმიერი პოლინომიური მნიშვნელობის d, კომიტერისა და გადამოწმების პარამეტრებისთვის, რომლებიც მოწოდებულია Setup-დან და შეტყობინებები m და m', რომლებიც განსხვავდებიან მაქსიმუმ j-ურ კოორდინატში. ვალდებულებისა და მტკიცებულების განახლებამ ეფექტურად უნდა უზრუნველყოს შედეგები, რომლებიც შედარებულია შეცვლილი შეტყობინების ვექტორზე ახალი ვალდებულებისა და მტკიცებულების შექმნასთან. შედეგების მდგომარეობის შესახებ ინფორმაციის ჩართვა შესაძლებელს ხდის კომპოზიციურობას, რაც იძლევა მრავალრიცხოვან განახლებებს ექსპონენციურ საზღვრებში.

კომპაქტური და ეფექტური გადაწყვეტილებები მნიშვნელოვნად აღემატება ადრინდელ კვლევებს ფუნდამენტური ვარაუდის „ხარისხის“, გენერირებული გადაწყვეტილებების ეფექტურობის ან ორივეს თვალსაზრისით. თუმცა, მნიშვნელოვანია, რომ მიდგომები, რომლებიც წარმოიქმნება, დაგვიცვას კვანტური კომპიუტერული გამოწვევებისგან [15]. კვანტურ კომპიუტერებს ამჟამად შეუძლიათ გატეხონ RSA-ზე და სხვა პოპულარულ ასიმეტრიულ სისტემებზე დაფუძნებული ვექტორული ვალდებულებები. იმისათვის, რომ უფრო ეფექტური და უსაფრთხო გახდეს, მკვლევარები აძლიერებენ ვალდებულებებს გისოსების ანუ ლატისების გამოყენებით და ხელმოწერის სისტემების შემუშავებით, რომლებიც გამოიყენებენ ვერკლის ხეებს. ჩვენთვის მნიშვნელოვანია გვქონდეს სქემები, რომლებიც დამოკიდებულია პოსტკვანტურ დაშვებებზე.

6. ლატისებზე დაფუძნებული ვექტორული ვალდებულება

ვექტორულ ვალდებულებებს გააჩნიათ მრავალი კრიპტოგრაფიული გამოყენება, როგორიცაა კრიპტოვალუტები, კრიპტოგრაფიული აკუმულატორები და დამოწმებული გარე მონაცემთა ბაზები. თუმცა, მცირედ გვაქვს გამოკვლეული პოსტ–კვანტური ვექტორული ვალდებულების სქემები, რომლებიც დაცულია კვანტური შეტევებისგან. პოსტ–კვანტური ჰეშირების ფუნქციით აშენებული მერკლის ხეები შეიძლება გამოვიყენოთ, მაგრამ მათზე გავლენა აქვს საჭირო და შედარებით არაეფექტურ განახლებებს.

ეს სტატია წარმოადგენს stateless, განახლებად VC სქემას მერკლის ხის მსგავსი კონსტრუქციიდათ, რომელიც დაფუძნებულია SIS გისოსების/ლატისების პრობლემაზე [16]. ეს ვექტორული ვალდებულება უფრო ეფექტურია და გააჩნია არსებითად უფრო მოკლე მტკიცებულებები. კერძო გასაღების კონფიგურაციით, საჯარო პარამეტრების გენერირება ხდება ცენტრალური ხელისუფლების მიერ მისი შეფერხების დრომდე.

სქემის კონსტრუქცია იყენებს ვექტორულ სივრცეს M, სადაც შეტყობინებები არის ℓ ვექტორები და მიეკუთვნება მიმდებარე მთელი რიცხვების I ინტერვალს. მთელი რიცხვების მაქსიმალური სიდიდე I–ში აღინიშნება, როგორც M_I. Setup ალგორითმი აგენერირებს committer და გადამოწმების პარამეტრებს cp და vp, შემთხვევითი მატრიცის გამოყენებით $\overline{\mathrm{A}} \leftarrow \mathbb{Z}_q^{n\times m}$; ასრულებს TrapGen ალგორითმს A და T მატრიცების მისაღებად. ალგორითმი აყალიბებს A_i მატრიცებს და შემთხვევით მატრიცას U, სადაც თითოეული U_j არის $\mathbb{Z}_q^{n\times\ell}$. $\mathrm{R}_{i,j}$ მატრიცები მიღებულია SamplePre ალგორითმის გამოყენებით, რაც უზრუნველყოფს, რომ $\mathrm{H}_d - \mathrm{H}_i$ არის ინვერსიული. Setup ალგორითმის გამომავალი მნიშვნელობა არის $cp = \left(\mathrm{U}, \mathrm{R} = \left(\mathrm{R}_{i,j}\right)_{i,j\in[d]}\right)$, $vp = (\mathrm{A}, \mathrm{U})$.

Committer და open ალგორითმები ითვლის ვალდებულებას, მტკიცებულებას და შესრულებული შეტყობინების მდგომარეობას. ვერიფიკაციის ალგორითმი ამოწმებს პირობებს $\|\mathrm{p}_i\| \le \gamma$, და $\mathrm{c} = \mathrm{A}_i\mathrm{p}_i + \mathrm{U}_i\mathrm{m}_i$, არის უსაფრთხოების პარამეტრი. თუკი პირობები დაკმაყოფილებულია, ალგორითმი მიიღებს მტკიცებულებას, წინააღმდეგ შემთხვევაში ის უარყოფს მას.

ჩვენ ასევე გვაქვს განახლების ალგორითმები ვალდებულებების, მტკიცებულებებისა და მდგომარეობის შესაცვლელად.

PrepareUpdates ^{diff} - ეს ალგორითმი იღებს committer პარამეტრებს cp, ინდექსს j და განსხვავებას $\sigma \in \mathbb{Z}^{\ell}$. იგი წარმოქმნის ვალდებულების განახლებას σ_{pr}, მტკიცებულების განახლებას σ_{pr}, და მდგომარეობის განახლებას σ_{s}. აუცილებელია შეიცვალოს შესრულებული შეტყობინების ვექტორი.

UpdateC - გადამოწმების პარამეტრების vp, ვალდებულების c და ვალდებულების განახლების σ_{c} გათვალისწინებით, ეს ალგორითმი დეტერმინისტულად ითვლის განახლებულ ვალდებულებას c'.

UpdateP - ვერიფიკაციის პარამეტრების vp, ინდექსი i, მტკიცებულება $\mathrm{pr_i}$ და მტკიცებულების განახლება σ_{pr}-ის გათვალისწინებით, ეს ალგორითმი დეტერმინისტულად წარმოქმნის განახლებულ მტკიცებულებას $\mathrm{pr}_{\mathrm{i}}'$.

UpdateS - მოცემული გვაქვს committer პარამეტრები cp, მისი მდგომარეობა st, და მდგომარეობის განახლება σ_{s}. ეს ალგორითმი დეტერმინისტულად აწარმოებს committer–ის განახლებულ მდგომარეობას st'.

განახლების ალგორითმები გარანტიას იძლევა სქემის სიზუსტის და უსაფრთხოების, რაც უზრუნველყოფს უსაფრთხო ვალდებულებას, მტკიცებულებების გახსნას, გადამოწმებასა და მოდიფიკაციებს შეტყობინებების committed ვექტორებისთვის.

7. ახალი სქემა ვერკლის ხის გამოყენებით

ერთჯერადი ხელმოწერის სქემების განხორციელება და გამოყენება რთულია, რადგან საჭიროა ცალკეული გასაღების წყვილების ხელმოწერის შექმნა თითოეული მესიჯისთვის. გვჭირდება შევინახოთ n დაიჯესტები, რაც რთულად გამოსაყენებელს ხდის ერთჯერად ხელმოწერის სქემებს. ამის გადასაჭრელად იყენებენ მერკლის ხეს. ეს მიდგომა ცვლის რამდენიმე ვერიფიკაციის გასაღებს ერთი საჯარო გასაღებით, ოროზითი ხის გამოყენებით, როგორც ფესვი. მერკლის ხე სწრაფად ითვლება და შეგვიძლია შევქმნათ დიდი მერკლის მტკიცებულებები, მაგრამ მათი გამოყენებით ჩვენს ლოკალურ სივრცეზე მნიშვნელოვანი დატვირთვა აქვს.

ვერკლის ხეები, რომლებიც იძლევა უფრო მცირე ზომის მტკიცებულების საშუალებას, შეგვიძლია გამოვიყენოთ მერკლის ხის მაგივრად. ის არის გაუმჯობესებული და უფრო ეფექტური. შემმოწმებელმა მხოლოდ უნდა წარმოადგინოს ერთი მტკიცებულება, რომელიც აჩვენებს ყველა მშობელსა და შვილს ურთიერთობას. ამან შეიძლება შეამციროს მტკიცებულების ზომები 6-8-ით და 20-30-ით ან მეტით, ვიდრე იდეალური მერკლის ხეები და მერკლის Patricia ხეები.

ჩვენ ვიყენებთ ვერკლის ხეს მერკლის ხის ნაცვლად. ხელმომწერი ირჩევს $H \in \mathbb{N}, H \geq 2$ გასაღების წყვილის ფორმირებისას. ამის შემდეგ გასაღების წყვილი იქმნება, რომელთა გამოყენებით შეგვიძლია ხელი მოვაწეროთ და დავამოწმოთ 2^H დოკუმენტი. ხელმომწერი გამოიმუშავებს 2^H უნიკალურ გასაღების წყვილს $(X_j, Y_j), 0 \leq j < 2^H$. ამ შემთხვევაში ხელმოწერის გასაღები არის X_j , ხოლო ვერიფიკაციიის გასაღები კი Y_j. ორივე მათგანი ბიტების სტრიქონებია. ვერკლის ხის ფოთლებია $g(Y_j)$, $0 \leq j < 2^H$. როგორც ხის ფოთლები, ისინი გამოითვლება და გამოიყენება, და ყოველი კვანძი არის ჰეშის მნიშვნელობა, რომელიც წარმოიქმნება მისი შთამომავლების ჰეშების შეერთებით. ვერკლის ხის ფესვი ვალდებულება კრიპტოგრაფიის სქემაში არის საჯარო გასაღები. საჯარო გასაღების შესაქმნელად საჭიროა გამოვიყენოთ 2^H უნიკალური გასაღების წყვილი.

ხელმოწერების შექმნა შეგვიძლია ერთჯერადი ხელმოწერის გასაღებების გენერირებით. სანამ M-იდან აღებულ შეტყობინებას მოვაწერთ ხელს, უნდა გამოვთვალოთ n ბიტიანი დაიჯესტი $d = g(M)$. პირველად, n ზომის შეტყობინება იქმნება m ზომის შემთხვევითი ზომის შეტყობინებისგან, ჰეშირების ფუნქციის გამოყენებით, კონვერტირებით. დოკუმენტის ხელმოწერა შეიქმნება ძირეული ვალდებულების, ერთჯერადი ხელმოწერის, ერთჯერადი გადამოწმების გასაღების და ბოლოს, მტკიცებულების ინდექსის s-ის კომბინაციით.

ვერკლის ხელმოწერის ვერიფიკაცია შემდეგნაირად მუშაობს: $sign$–ის ერთჯერადი ხელმოწერა უნდა იყოს დამოწმებული Y_s–ით. თუ ეს მართალია, the VC_i ვალდებულებები

დამოწმებულია. ხელმოწერა დადასტურებულია, თუ ხის ფესვი უდრის ფესვის ვალდებულებას. ვერკლის ხის გათვალისწინებით, ფესვის ვალდებულება არის d.

8. ექსპერიმენტები

მერკლის ხე არის ძალიან სწრაფი და $O(n)$ ცრის მისი გამოთვლითი დრო. სამწუხაროდ, მათი მტკიცებულების ზომა $O(\log_2 n)$ შედარებით დიდია და შეიძლება გამოიწვიოს მნიშვნელოვანი სიგანის (width) ხარჯი. მათი მტკიცებულებების ზომა $O(w \log_w n)$ რეალურად უფრო დიდია ვიდრე ისეთი მერკლის ხე, რომელსაც უფრო დიდი სიგანე გააჩნია (w-ary ხეები). ვექტორული ვალდებულების სქემის გამოყენება ამცირებს მტკიცებულების ზომას ფიქსირებულ მნიშვნელობამდე – $O(1)$. თუმცა, ვექტორული ვალდებულების კონსტრუქცია არის ძალიან ძვირი და შრომატევადი, რაც მოითხოვს $O(n^2)$ გამოთვლას.

ვერკლის ხის სიგანე (width) w, მოითხოვს მხოლოდ $O(wn)$ დროს კონსტრუქციისთვის. გარდა ამისა, მერკლის ხის წევრობის მტკიცებულებებთან შედარებით, მისი მტკიცებულების ზომა არის მხოლოდ $O(\log_w n)$, რაც მნიშვნელოვნად ნაკლებია $O(\log_2 w)$. ჩვენთვის ეს კარგი გაცვლაა.

სქემა	კონსტრუქცია	განახლება	მტკიცებულების ზომა
მერკლის ხე	$O(n)$	$O(\log_2 n)$	$O(\log_2 n)$
მერკლის ხე (w-ary)	$O(n)$	$O(w\log_w n)$	$O(w\log_w n)$
ვექტორული ვალდებულება	$O(n^2)$	$O(n)$	$O(1)$
ვერკლის ხე	$O(\mathrm{w}n)$	$O(w\log_w n)$	$O(\log_w n)$

ფიგურა 2. სქემის შედარება

როგორც ვთქვით, პოსტკვანტური ვექტორული ვალდებულების სქემები შეზღუდულად არის გამოკვლეული, მხოლოდ მერკლის ხის მსგავსი კონსტრუქციები გვაქვს stateless არმქონე განახლებულ VC სქემებისთვის. ეს მეთოდები გადამწყვეტია კვანტური კომპიუტერის შეტევებისგან დასაცავად, რადგან კვანტურ კომპიუტერებს შეუძლიათ გატეხონ RSA-ზე დაფუძნებული ვექტორული ვალდებულებები. ხელმოწერის ტექნიკა იყენებს ვერკლის ხეს, მაგრამ ვექტორული ვალდებულებები აგებულია გისოსების/ლატისების გამოყენებით. ასევე

გვაქვს სხვა, პოსტკვანტური მერკლის ალგორითმები, როგორიცაა Fractal Merkle ალგორითმი [17].

ამ შემთხვევაში, კლასიკური ალგორითმის შედეგებია:

გასაღების გენერირების დრო- 0.049351, ხელმოწერის დრო - 0.0002425, ვერიფიკაციის დრო - 0.0038651.

Thread-ზე დაფუძნებული ალგორითმი:

გასაღების გენერირების დრო - 0.013841, ხელმოწერის დრო - 0.0002425, ვერიფიკაციის დრო - 0.0038651.

ჩვენ შევიმუშავეთ ვექტორული ვალდებულების ახალი პროტოკოლი, რომელიც ეფუძნება პოსტკვანტურ Short Integer Solution ლატისების პრობლემას. პროტოკოლი საშუალებას გვაძლევს ვექტორული შეტყობინებები გადავამოწმოთ და გვქონდეს უსაფრთხო ვალდებულება, დაწყებული stateless განახლებადი VC კონსტრუქციით. ეს განსაკუთრებით შესაფერისია დიდი განზომილების d-სთვის, საჯარო პარამეტრების კვადრატული დამოკიდებულების გამო. ხის სპეციალიზებული ტრანსფორმაცია გათვალისწინებულია უფრო დიდი ზომებისთვის, stateless განახლებების შენარჩუნებით და ლაკონური მტკიცებულებების უზრუნველსაყოფად. მეთოდის მთავარი უპირატესობა არის თეორიული უსაფრთხოება კვანტური თავდასხმებისგან, მაგრამ მას აქვს ლოგარითმული ვალდებულების და მტკიცებულების ზომების შედარება ვექტორულ განზომილებაში d. მიუხედავად ამისა, ლატისებზე დაფუძნებული კონსტრუქცია მკაცრად არის გამოცდილი კლასიკური ალგორითმების წინააღმდეგ, რის შედეგადაც უფრო მცირე ციფრული ხელმოწერა მივიღეთ, ვიდრე მერკლის ხის ვერსიასთან შედარებით.

ჩვენ გამოვცადეთ ალგორითმი იმავე აპარატზე, სადაც გავტესტეთ ელექტრონული ხელმოწერა, რომელიც მერკლის ხის საფუძველზეა შექმნილი.

მივიღეთ შემდეგი შედეგები:

გასაღების გენერირების დრო - 0.049351, ხელმოწერის დრო - 0.00001520, ვერიფიკაციის დრო - 0.00048250.

ჩვენი ლატისებზე დაფუძნებული კონსტრუქცია, რა თქმა უნდა, უფრო ნელია, მაგრამ ჩვენს შემთხვევაში ელექტრონული ხელმოწერა გაცილებით მეტია, ვიდრე მერკლის ხის ვერსიის შემთხვევაში.

ჩვენი ახალი ვექტორული ვალდებულების კონსტრუქცია, რომელიც დაფუძნებულია პოსტკვანტურ Short Integer Solution ლატისების პრობლემაზე, წარმოადგენს რეალურ ალტერნატივას, განსაკუთრებით იმ სცენარებში, სადაც კვანტური უსაფრთხოება უმთავრესია. ვალდებულებისა და მტკიცებულების ზომებში ურთიერთდამოკიდებულება საგულდაგულოდ არის დაბალანსებული და ემპირიული შედეგები ხაზს უსვამს ჩვენი მიდგომის პრაქტიკულ სარგებელს.

9. დასკვნა

გამოვიკვლიეთ ინსტრუმენტებს კლასიკური და კვანტური კრიპტოგრაფიისთვის, მათ შორის პოსტკვანტური კრიპტოგრაფიის სისტემები, ჰეშირებაზე დაფუძნებული ცალმხრივი ფუნქციები და მათი ინტეგრაცია მერკლის და ვერკლის ხეებში. ასევე განვიხილეთ ვექტორული ვალდებულებები და ლატისებზე დაფუძნებულ ვალდებულებებს. ახალი სქემების ეფექტურობამ განაპირობა ახალი მოდელის შექმნა და მისი ინტეგრაცია ვერკლის ხეებში, რაც ეფექტრურობას ზრდის.

შედეგად მიღებულმა სქემებმა უნდა დაიცვან სისტემები, როგორც ტრადიციული, ასევე კვანტური კომპიუტერების თავდასხმებისგან. მერკლის ხე, აგებული კრიპტოგრაფიული ჰეშის ფუნქციებით, უზრუნველყოფს ძლიერ დაცვას კვანტური შეტევებისგან. ვერკლის ხის მოდელი, რომელიც წარმოადგენს მერკლის სქემის გაუმჯობესებას, იძლევა მცირე ვერიგიკაციის საშუალებას, გვაძლევს მხოლოდ ერთი მტკიცებულების მოთხოვნით ყველა მშობლისა და შთამომავლის ურთიერთობა დავადასტუროთ, ვერიფიკაციის ზომის ეს შემცირება დაახლოებით 6-8-ჯერ არის მერკლის ჩვეულებრივ მიდგომასთან შედარებით.

ვერკლის ხეს ვიყენებთ მერკლის ხის ნაცვლად. ეს გაუმჯობესებულია, რომელიც მოითხოვს ვექტორის ვალდებულებას, როგორც მტკიცებულებას. ხელმოწერის მეთოდები იყენებს ვერკლის ხეებს და სისტემები მოქმედებენ პოსტკვანტური ვარაუდებით. კვლევა მიზნად ისახავს სისტემის უფრო უსაფრთხო და ეფექტური გახადოს, რაც უზრუნველყოფს, რომ მიღებული მეთოდები დაგვიცავს კვანტური კომპიუტერის შეტევებისგან.

10. დადასტურება/აღიარება

კვლევა [STEM – 22 -1076] განხორციელდა შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით.

ბიბლიოგრაფია

1. Chen, Lily, et al. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.
2. Buchmann, J., Dahmen, E., Szydlo, M. (2009). Hash-based Digital Signature Schemes. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_3
3. Biswas, Bhaskar, and Nicolas Sendrier. "McEliece cryptosystem implementation: Theory and practice." Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17-19, 2008 Proceedings 2. Springer Berlin Heidelberg, 2008.
4. Yin, X.; He, J.; Guo, Y.; Han, D.; Li, K.-C.; Castiglione, A. An Efficient Two-Factor Authentication Scheme Based on the Merkle Tree. Sensors 2020, 20, 5735. https://doi.org/10.3390/s20205735
5. Chen, Y.-C.; Chou, Y.-P.; Chou, Y.-C. An Image Authentication Scheme Using Merkle Tree Mechanisms. Future Internet 2019, 11, 149. https://doi.org/10.3390/fi11070149
6. Lamport, Leslie. "Constructing digital signatures from a one way function.",1979.

7. Post-Quantum Digital Signatures with Attenuated Pulse Generator; M. Iavich, R. Bocu, A. Arakelian, G. Iashvili; ceur-ws.org, Vol-2698, 2020.
8. Koo, D.; Shin, Y.; Yun, J.; Hur, J. Improving Security and Reliability in Merkle Tree-Based Online Data Authentication with Leakage Resilience. Appl. Sci. 2018, 8, 2532. https://doi.org/10.3390/app8122532
9. Sim, M.; Eum, S.; Song, G.; Yang, Y.; Kim, W.; Seo, H. K-XMSS and K-SPHINCS+: Enhancing Security in Next-Generation Mobile Communication and Internet Systems with Hash Based Signatures Using Korean Cryptography Algorithms. Sensors 2023, 23, 7558. https://doi.org/10.3390/s23177558
10. Merkle, R.C. (1988). A Digital Signature Based on a Conventional Encryption Function. In: Pomerance, C. (eds) Advances in Cryptology — CRYPTO ’87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48184-2_32
11. Chen, H.; Liang, D. Adaptive Spatio-Temporal Query Strategies in Blockchain. ISPRS Int. J. Geo-Inf. 2022, 11, 409. https://doi.org/10.3390/ijgi11070409
12. Weijie Wang, Annie Ulichney, and Charalampos Papamanthou. 2023. BalanceProofs: maintainable vector commitments with fast aggregation. In Proceedings of the 32nd USENIX Conference on Security Symposium (SEC '23). USENIX Association, USA, Article 247, 4409–4426.
13. Kurosawa, Kaoru, and Goichiro Hanaoka, eds. Public-Key Cryptography--PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, Feburary 26--March 1, 2013, Proceedings. Vol. 7778. Springer, 2013.
14. Peikert, Chris, Zachary Pepin, and Chad Sharp. "Vector and functional commitments from lattices." In Theory of Cryptography: 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part III 19, pp. 480-511. Springer International Publishing, 2021.
15. Kuszmaul, John. “Verkle Trees.”, 2019
16. C. Papamanthou, E. Shi, R. Tamassia, and K. Yi. Streaming authenticated data structures. In EUROCRYPT, pages 353–370. 2013.
17. Iavich, M., Gnatyuk, S., Arakelian, A., Iashvili, G., Polishchuk, Y., & Prysiazhnyy, D. (2021). Improved Post-quantum Merkle Algorithm Based on Threads. In Advances in Computer Science for Engineering and Education III 3 (pp. 454-464). Springer International Publishing.