Scientific and Practical Cyber Security Journal (SPCSJ) 6(3): 50-56 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

პოსტ-კვანტური ხელმოწერის დიზაინის საწყისი კონცეფციები Verkle-ის ხის გამოყენებით

THE INITIAL CONCEPTS OF POST-QUANTUM SIGNATURE DESIGN USING VERKLE TREE

მაქსიმ იავიჩი, სამეცნიერო კიბერუსაფრთხოების ასოციაცია, კავკასიის უნივერსიტეტი
Maksim Iavich, Scientific cyber security association, Caucasus University
ავთანდილ გაგნიძე, სამეცნიერო კიბერუსაფრთხოების ასოციაცია, აღმოსავლეთ ევროპის უნივერსიტეტი
Avtandil Gagnidze, Scientific cyber security association, East European University
გიორგი იაშვილი, სამეცნიერო კიბერუსაფრთხოების ასოციაცია, კავკასიის უნივერსიტეტი
Giorgi Iashvili, Scientific cyber security association, Caucasus University

რეზიუმე: ნაშრომში აღწერილია ჰეშზე დაფუძნებული პოსტკვანტური ციფრული სქემები. გაანალიზებულია ციფრული ხელმოწერები Merkle-ს ხეზე დაყრდნობით. ნაშრომის ავტორები გვთავაზობენ ციფრული ხელმოწერის დიზაინის მეთოდოლოგიას ახალი ტექნოლოგიის, Verkle-ს ხის გამოყენებით. ისინი ასევე გვთავაზობენ პოსტ-კვანტური ხელმოწერის დიზაინის კონცეფციებს Verkle-ის ხის გამოყენებით.

საკვანძო სიტყვები: პოსტ-კვანტური, Verkle-ს ხე, Merkle-ს ხე, ციფრული ხელმოწერა, პოსტკვანტური ხელმოწერის დიზაინი, გასაღების გენერაცია, ხელმოწერის გენერაცია, ხელმოწერის ვერიფიკაცია

ABSTRACT: *The paper describes post-quantum hash-based digital schemes. It analyzes digital signatures based on Merkle tree. The authors of the papers offer the methodology of designing the digital signature using the novel technology, Verkle tree. They also offer the concepts of post-quantum signature design using Verkle Tree.*

KEYWORDS: *post-quantum, Verkle Tree, Merkle Tree, igital signature, post-quantum signature design, Key generation, Signature generation, Signature verification*

შესავალი

ბოლო დროს მსოფლიოს წამყვანი მეცნიერები და ინჟინრები დაუღალავად მუშაობენ კვანტური კომპიუტერების შექმნაზე. აღიარებული ლიდერები კვანტური კომპიუტერების განვითარებაში Google Corporation, Universities Space Research Association, federal agency NASA და D-WAVE, უკვე მზად არიან გარღვევის მოსახდენად კვანტური ტექნოლოგიის სფეროში. 2019 წლის ოქტომბერში Google-მა განაცხადა, რომ მიაღწია კვანტურ უზენაესობას, რამაც სერიოზული კამათი გამოიწვია, მაგრამ თუ გავითვალისწინებთ იმ ფაქტს, რომ ტექნიკური გიგანტები იბრძვიან პირველი კვანტური კომპიუტერების შესაქმნელად და მათ მნიშვნელოვან წარმატებებსაც მიაღწიეს ამ მიმართულებით, მსოფლიო შეიძლება დადგეს ახალი ეპოქის

ზღვარზე. Google თვლის, რომ მისი ამჟამინდელი ჩიპის დიზაინს შეუძლია გაზარდოს მეხსიერების მოცულობა 100-დან 1000 კუბიტამდე. IBM მას ფეხდაფეხ მოსდევს, რადგან ამტკიცებს, რომ 2023 წლის ბოლოსთვის შექმნის 1000 კუბიტზე მეტი სიმძლავრის და დაახლოებით 10-დან 50 ლოგიკურ კუბიტამდე სიმძლავრის კვანტურ პროცესორს. მან 2021 წელს უკვე წარმოადგინა 127 კუბიტიანი, ხოლო 2022 წელს 433 კუბიტანი პროცესორი. ჩინელი მეცნიერები ამტკიცებენ, რომ "Zuchongzhi 2" - 66 კუბიტიანმა კვანტურმა პროცესორმა, დავალება Google-ის პროცესორთან შედარებით 1 მილიონჯერ უფრო სწრაფად შეასრულა. ეს პროცესორი შეიქმნა ჩინეთის მეცნიერებათა აკადემიის კვანტური ინფორმაციისა და კვანტური ფიზიკის მოწინავე გამოცდილების ცენტრის მკვლევართა გუნდის მიერ შანხაის ტექნიკური ფიზიკის ინსტიტუტთან და შანხაის მიკროსისტემისა და საინფორმაციო ტექნოლოგიების ინსტიტუტთან ერთად [1-5].

დაბოლოს, კვანტური კომპიუტერები შეძლებენ დღეისათვის არსებული კრიპტოგრაფიული კოდების გატეხვას, რომლებიც გამოიყენება კომუნიკაციებისა და ფინანსური ტრანზაქციებისთვის, ასე რომ, ამჟამად გამოყენებული ციფრული ხელმოწერის სისტემები უძლურია კვანტური კომპიუტერებით განხორციელებული თავდასხმების მიმართ, ამიტომ მსოფლიომ უნდა მიიღოს კვანტურ-რეზისტენტული კრიპტოგრაფია. ამჟამად გამოყენებული ციფრული ხელმოწერის სისტემების უსაფრთხოება ემყარება დისკრეტული ლოგარითმების გაანგარიშების პრობლემას და დიდი რიცხვების ფაქტორიზაციას. ზოგიერთი კრიპტოსისტემა, მაგალითად RSA - ოთხი ათასი ბიტიანი გასაღებით, გამოსადეგია კლასიკური კომპიუტერით განხორციელებული შეტევების წინააღმდეგ, მაგრამ აბსოლუტურად უსარგებლოა კვანტური კომპიუტერების მიერ განხორციელებული შეტევების წინააღმდეგ.

დღისათის RSA კრიპტოსისტემა თითქმის ყოველ ნაბიჯზე გამოიყენება, რადგან მას იყენებს მრავალი მსხვილი ორგანიზაცია, მაგალითად, სამთავრობო დაწესებულებები, ბანკები, კორპორაციების უმეტესობა, სამთავრობო ლაბორატორიები და უნივერსიტეტები. გარდა ამისა, ეს კრიპტოსისტემა გამოიყენება კომერციულ პროდუქტებში, ოპერაციულ სისტემებში, Ethernet-ში, ქსელურ ბარათებში, სმარტ ბარათებში და ასევე გამოიყენება კრიპტოგრაფიულ აპარატურაში. RSA BSAFE დაშიფვრის ტექნოლოგიას დაახლოებით 500 მილიონი მომხმარებელი ჰყავს, რომელთა რიცხვი სწრაფად იზრდება. RSA ალგორითმი არის ერთ-ერთი ყველაზე გავრცელებული საჯარო გასაღების კრიპტოსისტემა. ამიტომ RSA-ს გატეხვამ შეიძლება სრული ქაოსი გამოიწვიოს. მეცნიერები თვდაუზოგავად მუშაობენ RSA-ს ალტერნატივების შესაქმნელად, რომელიც კვანტური კომპიუტერების თავდასხმებს გაუძლებს. RSA-ს ალტერნატივად ჩვენ შეგვიძლია განვიხილოთ კრიპტოგრაფიულ ჰეშ ფუნქციაზე დაფუძნებული ციფრული ხელმოწერის ჰეშ სქემები. ჰეშ ფუნქციის კოლიზიისადმი მედეგობა არის ამ ხელმოწერის უსაფრთხოების გარანტი.

1. ჰეშზე დაფუძნებული ციფრული ხელმოწერის სქემა:

Lamport–Diffie-ის მიერ შემოთავაზებული ჰეშზე დაფუძნებული ერთჯერადი ხელმოწერის სქემა, განიხილება, როგორც ციფრული ხელმოწერის ალტერნატიული სქემა პოსტკვანტური ეპოქისთვის. ჩვენ ვხედავთ, რომ გასაღები და ხელმოწერის გენერირება ეფექტურია Lamport–Diffie-ის ერთჯერადი ხელმოწერის სქემაში, მაგრამ ხელმოწერის ზომა უდრის n2-ს, სადაც ჰეშირებული ბადის ზომა არის n, რაც საკმაოდ დიდია. Winternitz-ის მიერ შემოთავაზებული ერთჯერადი ხელმოწერის სქემა მნიშვნელოვნად ამცირებს ხელმოწერის ზომას, რადგან ამ სქემაში შეგვიძლია ერთი სტრიქონიანი გასაღების გამოყენება ჰეშირებული შეტყობინების რამდენიმე ბიტის ხელმოსაწერად [5], მაგრამ, ამ შემთხვევაში პრობლემის წინაშე ვდგებით, როდესაც ვიყენებთ ერთჯერადი ხელმოწერის სქემას გასაღებების დიდი რაოდენობის გასაცვლელად, რადგან ის იყენებს სხვადასხვა გასაღების წყვილს ყოველი შეტყობინებისთვის. ამ პრობლემის გადასაჭრელად Merkle-ის ციფრული ხელმოწერის სქემა იყენებს ოროობით ხეს, რათა თავიდან აიცილოს ვერიფიკაციის გასაღებების დიდი რაოდენობის გამოყენება ერთ საჯარო გასაღებთან. საჯარო გასაღები აქ არის ამ ხის ფესვი [6-12].

გასაღების გენერაცია: ხის სიგრძე არჩეულია როგორც H>=2. აქ ერთ საჯარო გასაღებს შეუძლია ხელი მოაწეროს 2H რაოდენობის დოკუმენტს. იქმნება 2H გასაღების წყვილი Xi და Yi, სადაც Xi არის ხელმოწერის გასაღები და Yi ვერიფიკაციის გასაღები, h (Yi) გამოითვლება და გამოიყენება ხის ფოთლებად. ხის თითოეული განშტოება არის მისი შვილების კონკატენაციის ჰეშ მნიშვნელობა.

a[1,0]=h(a[0,0] || a[0,1])

Merkle-ის კრიპტო სქემის საჯარო გასაღები არის ოროობითი ხის ფესვი, მის შესაქმნელად საჭიროა 2H წყვილი ერთჯერადი გასაღების გამოთვლა.

ხელმოწერის გენერირება: რენდომული ზომის შეტყობინება m, გარდაიქმნება n ზომის შეტყობინებად ჰეშის ფუნქციის საშუალებით. h (m) = ჰეში, და იქმნება ერთჯერადი ხელმოწერა რენდომული ერთჯერადი გასაღების Xarb-ის გამოყენებით, დოკუმენტის ხელმოწერა იქნება: ერთჯერადი ხელმოწერის, ერთჯერადი ვერიფიკაციის გასაღები Yarb, ინდექსის arb და ყველა "authi" მონათესავე ტოტის შეერთება Yarb- თან მიმართებაში.

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

ხელმოწერის დადასტურება: Merkle-ის კრიპტო-სისტემის ხელმოწერის დამადასტურებელ ხელმოწერაში, sig-ის ერთჯერადი ხელმოწერა უნდა გადამოწმდეს Yarb-ის გამოყენებით, იმ შემთხვევაში თუ ეს სწორი იქნება, ყველა კვანძი a [i, j] გამოითვლება "authi", ინდექსის arb და Yarb გამოყენებით. თუ ხის ფესვი უდრის საჯარო გასაღებს, მაშინ ხელმოწერა სწორია.

2. Verkle vs Merkle

Verkle-ს ხეები არის Merkle-ს ხეების ძლიერი განახლება, რაც იძლევა ბევრად უფრო მცირე ზომის ვერიფიკაციის გამოყენების საშუალებას და უფრო ეფექტურია. Verkle-ს ხის სტრუქტურა ძალიან ჰგავს Merkle Patricia ხეს [13, 14].

სურათზე 1, აგებულია Verkle-ს ხე 9 ფაილისგან, სადაც განშტოების კოეფიციენტი არის 3. ფაილების k = 3 ზომის ქვეჯგუფებად დაყოფის შემდეგ, თითოეულ ქვეჯგუფზე გამოითვლება ვექტორის ვალდებულება შესაბამისი წევრობის მტკიცებულებებთან ერთად. ეს გვაძლევს ვალდებულებებს VC1, VC 2 და VC3. ვექტორული ვალდებულება VC4 გამოითვლება ამ სამ ვალდებულებასთან ერთად წევრობის მტკიცებულებებთან ერთად p9, p10 და p11 ვალდებულებებისთვის VC1, VC2 და VC3 შესაბამისად VC4 ვალდებულების მიმართ. Verkle-ს ხის საბოლოო გადაწყვეტა არის ძირეული ვალდებულება, რომელიც ამ შემთხვევაში არის VC4.

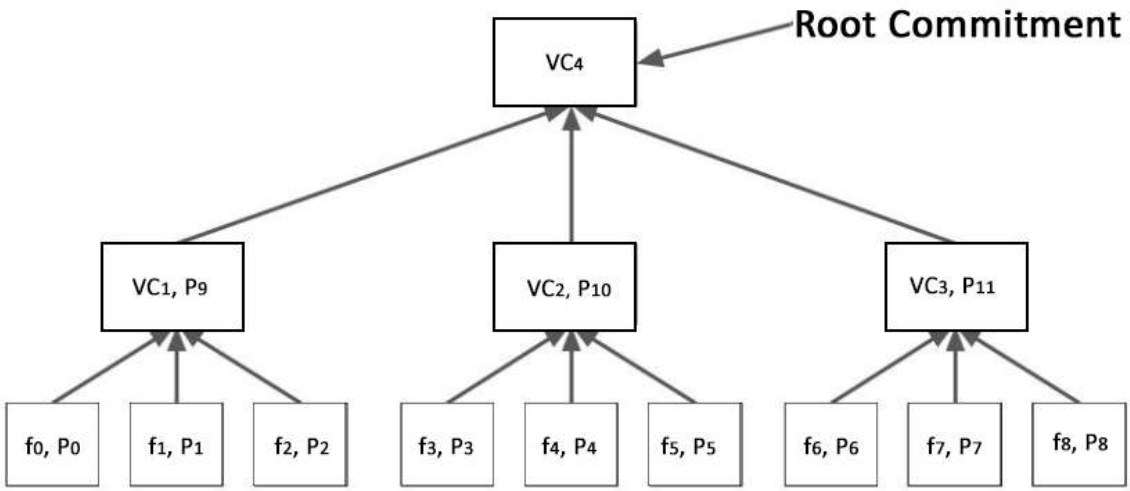

Fig1. Verkle Tree

Merkle-ს ხეში, მნიშვნელობის მტკიცებულება შედგება frlattern კვანძების მთელი ნაკრებისგან: მტკიცებულება უნდა შეიცავდეს ხეში არსებულ ყველა კვანძს, რომელსაც ყავს საერთო მშობელი ნებისმიერ კვანძთან იმ გზაზე, რომელიც მიდის დასადასტურებელ კვანძამდე.

ამ მიზეზით ხელმოწერა ძალიან გრძელი გამოდის. ჩვენ უნდა მივაწოდოთ frlattern კვანძები თითოეულ დონეზე, რადგან ჩვენ გვჭირდება შვილობილი კვანძის მთელი ნაკრები ამ კვანძის მნიშვნელობის გამოსათვლელად და ჩვენ უნდა გავაგრძელოთ ეს მანამ, სანამ არ მივაღწევთ ხის ფესვამდე.

მეორეს მხრივ, Verkle-ს ხეში ჩვენ არ გვჭირდება flattern კვანძების მიწოდება; ვინაიდან აქ, ჩვენ მხოლოდ ბილიკს ვუთითებთ. ამიტომაა, რომ Verkle-ს ხეები არის განიერი, ხოლო Merkle Patricia ხეები არა: უფრო დიდი სიგანის ხე ორივე შემთხვევაში უფრო მოკლე ბილიკამდე მიდის, მაგრამ Merkle Patricia ხეში ეს ეფექტი გადალახულია მთელი სიგანის მიწოდების საჭიროების მაღალი ღირებულებით. - 1 flattern კვანძი თითო მტკიცებულების განშტოებაზე.

Verkle-ს ხეში არ გვაქვს მსგავსი ეფექტურობის პრობლემა, რაც მას ბევრად უფრო ეფექტურს ხდის.

3. ახალი სქემა

Verkle-ს ძირეული ვალდებულება არის საჯარო გასაღები. იხილეთ ნახ. 2

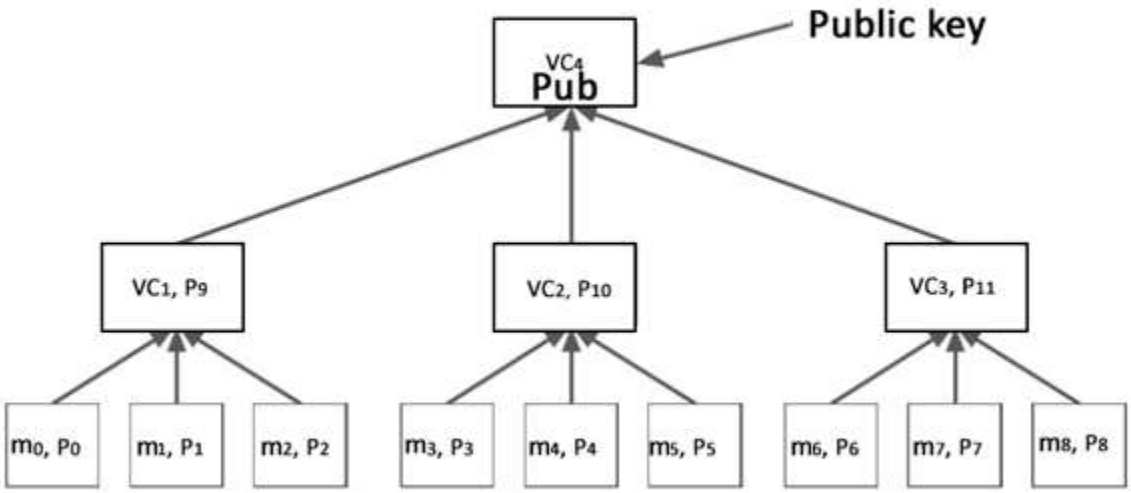

Fig 2. Verkle Signature Scheme

გასაღების გენერაცია: ხის სიგრძე არჩეულია როგორც H>=2. აქ ერთ საჯარო გასაღებს შეუძლია ხელი მოაწეროს 2H რაოდენობის დოკუმენტს. იქმნება 2H გასაღების წყვილი Xi და Yi, სადაც Xi არის ხელმოწერის გასაღები და Yi ვერიფიკაციის გასაღები, h (Yi) გამოითვლება და გამოიყენება ხის ფოთლებად. ხის თითოეული კვანძი არის მისი განშტოებების შეერთების ჰეშ მნიშვნელობა.

a[1,0]=h(a[0,0] || a[0,1])

Verkle-ს კრიპტო სქემის საჯარო გასაღები არის ძირეული ვალდებულება, მის დაგენერირებისთვის უნდა გამოითვალოს 2H რაოდენობის წყვილი ერთჯერადი გასაღები.

ხელმოწერის გენერირება: რენდომული ზომის შეტყობინება m, გარდაიქმნება ზომად n ჰეშის ფუნქციის საშუალებით. h (m) = ჰეში, და იქმნება ერთჯერადი ხელმოწერა რენდომული ერთჯერადი გასაღების Xarb-ის გამოყენებით, დოკუმენტის ხელმოწერა იქნება: ერთჯერადი ხელმოწერა, ერთჯერადი გადამოწმების გასაღები Yarb, ინდექსის arb მტკიცებულება და

ძირეული ვალდებულება. ხელმოწერა= (sig||arb|| Yarb||მტკიცებულება, ძირეული ვალდებულება)
ხელმოწერის გადამოწმება: Verkle-ში ციფრული ხელმოწერის გადამოწმებაკეთდება შემდეგნაირად, sig-ის ერთჯერადი ხელმოწერა უნდა გადამოწმდეს Yarb-ის გამოყენებით, თუ ეს სწორი აღმოჩნდება, ყველა დადასტურება VC [i] გამოითვლება "authi", ინდექსის arb და Yarb გამოყენებით. თუ ხის ფესვი უდრის ფესვის ვალდებულებას, ხდება ხელმოწერის ვერიფიკაცია.

4. დასკვნები

Verkle სქემა არის Merkle-ის სქემის ძლიერი განახლება, რომელიც იძლევა ბევრად უფრო მცირე ზომის ვერიფიკაციის საშუალებას. ნაცვლად ყველა "auth კვანძის" უზრუნველყოფისა თითოეულ დონეზე, ვერიფიკაციას სჭირდება მხოლოდ ერთი მტკიცებულება, რომელიც დაადასტურებს ყველა მშობელი-მემკვიდრე ურთიერთობას - ყველა ვალდებულებას თითოეული ფოთლის კვანძიდან ფესვამდე. ეს საშუალებას იძლევა ვერიფიკაციის ზომები შემცირდეს დაახლოებით 6-8-ჯერ, კლასიკურ Merkle-ს სქემასთან შედარებით.

ეს მოითხოვს უფრო რთულ კრიპტოგრაფიას, მაგრამ ამავდროულად ეს გვაძლევს მასშტაბირების გაზრდის შესაძლებლობას. საშუალოვადიან პერსპექტივაში, SNARK-ებს შეუძლიათ კიდევ უფრო გააუმჯობესონ მდგომარეობა: ჩვენ შეგვიძლია გამოვიყენოთ SNARK უკვე ეფექტური Verkle proof Verifier-ი, რათა ვერიფიკაციის ზომა შევამციროთ თითქმის ნულამდე, ან დავუბრუნდეთ SNARKed Merkle-ის მტკიცებულებებს, თუ/როცა SNARK-ები ბევრად უკეთესი გახდება.

შემდგომში, კვანტური გამოთვლების ზრდა გვაიძულებს გადავიდეთ STARKed მტკიცებულებებზე ჰეშებით, რადგან ეს უკანასკნელი ხაზოვან ჰომორფიზმებს, რომლებზეც Verkle-ს ხეები არიან დამოკიდებულნი დაუცველს ხდის. მაგრამ ჯერჯერობით, ეს იგივე მოგებას გვაძლევს მასშტაბირების მხრივ, რასაც მივიღებდით უფრო მოწინავე ტექნოლოგიებით. ჩვენ უკვე გაგვაჩნია ყველა ინსტრუმენტი, რომელიც გვჭირდება ამ ყველაფრის ეფექტური განხორციელებისთვის.

პოლინომიური ვალდებულებების კვანტური უზრუნველყოფის სქემა უნდა შეიცვალოს პოსტკვანტურ დაშვებებზე დაფუძნებული სქემებით.

ბიბლიოგრაფია:

1. Ladd, T., Jelezko, F., Laflamme, R. et al. Quantum computers. Nature 464, 45–53 (2010). https://doi.org/10.1038/nature08812

2. Divincenzo, D.P. (1997). Topics in Quantum Computers. In: Sohn, L.L., Kouwenhoven, L.P., Schön, G. (eds) Mesoscopic Electron Transport. NATO ASI Series, vol 345. Springer, Dordrecht. https://doi.org/10.1007/978-94-015-8839-3_18

3. Gardas, B., Dziarmaga, J., Zurek, W.H. et al. Defects in Quantum Computers. Sci Rep 8, 4539 (2018). https://doi.org/10.1038/s41598-018-22763-2

4. Lele, A. (2021). Quantum Computers. In: Quantum Technologies and Military Strategy. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-72721-5_3

5. J. Bardin, "Beyond-Classical Computing Using Superconducting Quantum Processors," 2022 IEEE International Solid- State Circuits Conference (ISSCC), 2022, pp. 422-424, doi: 10.1109/ISSCC42614.2022.9731635.

6. Dods, C., Smart, N.P., Stam, M. (2005). Hash Based Digital Signature Schemes. In: Smart, N.P. (eds) Cryptography and Coding. Cryptography and Coding 2005. Lecture Notes in Computer Science, vol 3796. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11586821_8

7. 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

8. Rohde, S., Eisenbarth, T., Dahmen, E., Buchmann, J., Paar, C. (2008). Fast Hash-Based Signatures on Constrained Devices. In: Grimaud, G., Standaert, FX. (eds) Smart Card Research and Advanced Applications. CARDIS 2008. Lecture Notes in Computer Science, vol 5189. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-85893-5_8

9. M. Schneider and Shih-Fu Chang, "A robust content based digital signature for image authentication," Proceedings of 3rd IEEE International Conference on Image Processing, 1996, pp. 227-230 vol.3, doi: 10.1109/ICIP.1996.560425.

10. M. Iavich, G. Iashvili, R. Bocu and S. Gnatyuk, "Post-quantum digital signature scheme for personal data security in communication network systems", International Conference of Artificial Intelligence Medical Engineering Education, pp. 303-314, 2020.

11. Iavich, M., Gagnidze, A., Iashvili, G., Hash based digital signature scheme with integrated TRNG, CEUR Workshop Proceedings, 2018

12. Avtandil Gagnidze & Maksim Iavich & Giorgi Iashvili, 2017. "Some Aspects Of Post-Quantum Cryptosystems," Eurasian Journal of Business and Management, Eurasian Publications, vol. 5(1), pages 16-20.

13. 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

14. Weijie Wang, Yale University Annie Ulichney, Yale University Charalampos Papamanthou, Yale University, BalanceProofs: Maintainable Vector Commitments with Fast Aggregation, Cryptology ePrint Archive, 2022