Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 86-91 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

Digital signature in post-quantum computers epoch

ციფრული ხელმოწერა პოსტ-კვანტური კომპიუტერების ეპოქაში

Salome Tkhilaishvili
Caucasus University

ABSTRACT. Scientists say that in the near future the speed of computers will be significantly increased and quantum computers will be able to easily allocate the crypto keys of the set by the force method. Quantum computers will be able to easily calculate the numbers factorization operations, the problem with the system is based on RSA crypto system, this crypto system is the most common in the world, hence its break will cause damage to almost all product. So it will be required to create and further develop the algorithm by means of which we will create the system resistant to attacks of quantum computers. In the article is done the critical analysis of existing crypto systems. Are proposed the algorithms of hash based crypto systems and the evaluation is done.

KEYWORDS: quantum, post-quantum, digital signature

ABSTRACT. მეცნიერების ვარაუდით, ახლო მომავალში კომპიუტერის სისწრაფე საგრძნობლად გაიზრდება და კვანტური კომპიუტერი შიფრის გასაღებთა სიმრავლეს ძალისმიერი მეთოდით გადაარჩევს. კვანტურ კომპიუტერებს შეეძლებათ მარტივად გამოიანგარიშონ მარტივ რიცხვებზე ფაქტორიზაციის ოპერაციები, სწორედ ამ პრობლემაზე არის დაფუძნებული RSA კტიპტო სისტემა , ეს კრიპტო სისტემა არის დღესდღეობით ყველაზე მეტად გავრცელებული მსოფლიოში, აქედან გამომდინარე მისი გატეხვა გამოიწვევს თითქმის ყველა პროდუქტის დაზიანებას .შესაბამისად საჭირო გახდება შევქმნათ და შემდგომში დავხვეწოთ ალგორითმი რომლის საშუელებითაც შევქმნით კვანტური კომპიუტერის შეტევებისადმი მედეგ კრიპტოსისტემას. სტატიაში კეთდება არსებული კრიპტო სისტემების კრიტიკული ანალიზი. შემოთავაზებულია ჰოშზე დაფუძნებული კრიპტოს სისტემების ალგორითმები და გაკეთებულია შეფასება.

შესავალი

ციფრული ხელმოწერა თანდათან გახდა ინტერნეტისა და სხვადასხვა IT ინფრასტრუქტურის უსაფრთხოებისა და დაცულობის გარანტი. ის საკმაოდ აქტუალურია საქართველოშიც განსაკუთრებიდ მას შემდეგ, რაც საქართველოს

იუსტიციის სამინისტრომ დაიწყო ახალი პირადობის დამადასტურებელი დოკუმენტის ID ბარათის გაცემა ,რომელიც მოქალაქეს საშუალებას აძლევს ხელი მოაწეროს ნებისმიერ დოკუმენტს ციფრულად და ამ ხელმოწერას ისეთივე ფასი და ძალა ექნება როგორც ნამდვილ ხელნაწერს, ამავდროულად ციფრული ხელმოწერის გამოყენების შემთხვევაში მინიმუმამდეა დაყვანილი დოკუმენტების გაყალბება, სწორედ ამიტომ ის უკვე ფართოდ გამოიყენება მთელ რიგ სამთავრობო უწყებებსა და კერძო სექტორში როგორებიცაა:საბანკო სექტორი, სატელეკომუნიკაციო კომპანიები (მაგალითად ჯეოსელში) და მიკროსაფინანსო ორგანიზაციები(მაგალითად კრისტალი).დღესდღეობით პოპულარული ციფრული ხელმოწერის სქმებია:RSA,DSA,ECDSA ისინი ძირითადად ეყრდნობიან რთული რიცხვების ფაქტორიზაციასა და დისკრეტული ალგორითმის გამოთვლის სირთულეს ,მეცნიერთა ვარაუდით კი უახლოეს მომავალში კომპიუტერის სისწრაფე საგრძნობლად გაიზრდება და კვანტური კომპიუტერი შიფრის გასაღებთა სიმრავლეს ძალისმიერი მეთოდით გადაარჩევს.კვანტურ კომპიუტერებს შეეძლებათ მარტივად გამოიანგარიშონ მარტივ რიცხვებზე ფაქტორიზაციის ოპერაციები , სწორედ ამ პრობლემაზე არის დაფუძნებული RSA კტიპტო სისტემა , ეს კრიპტო სისტემა არის დღესდღეობით ყველაზე მეტად გავრცელებული მსოფლიოში, აქედან გამომდინარე მისი გატეხვა გამოიწვევს თითქმის ყველა პროდუქტის გატეხვას.სწორე ამიტომ ჩვენ მოგვიწევს შევქმნათ და შემდგომში დავხვეწოთ ალგორითმი,რომელიც შემდგომში საშუალებას მოგვცემს განვავითაროთ კვანტური კომპიუტერის შეტევებისადმი მედეგი კრიპტოსისტემა[1].

კვანტური კომპიუტერის შეტევების მიმართ ერთ-ერთი ყველაზე კრიპტომედეგი ხელმოწერის სქემაა მერკლის ხელმოწერის სქემა, რომელიც თავის მხრივ მოიცავს secure hash function და one time signature შესაბამისად დაცული და უსაფრთხო კრიპტოსისტემის შესაქმნელად მნიშვნელოვანია ისეთი ხელმოწერის სქემისა და ალგორითმების გამოყენება,რომლებიც უზრუნველყოფენ ოპტიმიზირებული ციფრული ხელმოწერის შექმნას .იმისთვის რომ შევქმნათ კრიპტომედეგი ციფრული ხელმოწერა მნიშვნელოვანია გავითვალისწონოთ: ერთჯერადი ხელმოწერის(one time signature) გასაღებების დაგენერირებისთვის საჭირო დრო და ხელმოწერისა და

ვერსიფიკაციისთვის საჭირო დრო.ლამპორტის ხელმოწერის სქემის გამოყენებისას მნიშვნელოვანია შევარჩიოთ ისეთი ცალმხრივი ჰეშ-ფუნქცია , რომელიც უზრუნველყოფს ერთჯერადი ციფრული ხელმოწერის უსაფრთხოებასა და საიმედოობას.მეტი თვალსაჩინოებისთვის განვიხილოთ ერთი მაგალითი როცა ლამპორტის ერთჯერადი ხელმოწერის შესაქმნელად გამოვიყენეთ კრიპტოგრაფიული ჰეშ-ფუნქცია $H:\{0,1\}^* \rightarrow H:\{0,1\}^8$ და შესაბამისად ხელი მოვაწეროთ M შეტყობინებას M=$(0,1)^k$ ამ შემთხვევაში ჩვენ შეგვეძლება ავირჩიოთ 2K ცალი შემთხვევით დაგენერირებული X_{ij} რიცხვი ამ დიაპაზონიდან $1 \leq i \leq k$, j={0,1} შესაბამისად ზემოთ ასახული მონაცემებიდან Y_{ij} არის ღია გასაღებების სიმრავლე, ხოლო X_{ij} არის დახურული გასაღებების სიმრავლე.ციფრული ხელმოწერის ღია გასაღები X (LD-OTS) შეიცავას 2n ცალ n სიმბოლოიან შემთხვევითი დაგენერირებით შერჩეულ ბიტურ ჩანაწერს სადაც X $\in R\{0,1\}^{(n,2n)}$ და $X = (x_{n-1}[0], x_{n-1}[1], \dots, x_1[0], x_1[1], x_0[0], x_0[1])$,ხოლო დახურული გასაღები კი ანალოგიურად შეიცავს შესაბამის Y_{ij} მნიშვველობებს სადაც $y_i[j] = f(x_i[j]),\ 0 \leq i \leq n-1, j = 0,1$ და $Y = (y_{n-1}[0], y_{n-1}[1], \dots, y_1[0], y_1[1], y_0[0], y_0[1]) \in R\{0,1\}^{(n,2n)}$.ასე რომ ლამპორტის ციფრული ხელმოწერის დაგენერირებისთვის დაგვჭირდება 2n ცალი n სიგრძის ბიტური სტიქონი.თავად ხელმოწერი პროცესი კი შემდეგნარად წარიმართება ავიღებთ შეტყობინებას M=$m_1,m_2,\dots m_k$ $m_i \in \{0,1\}$ და საიდუმლო გასაღებს (private key) X_{ij} სადაც $1 \leq i \leq k$ და j={0,1} ,შესაბამისად ყოველი i-ისთვის უნდა შევამოწმოთ m_i-ური მნისშვნელობა არის 0-ის ტოლი თუ 1-ის ტოლია , თუ ის ნულის ტოლია მაშინ ხელომოწერე ანუ sig $_i=X_{i0}$ ხოლო თუ ერთის ტოლია $sig_i=X_{i1}$ საბოლოაო ხელმოწერა კი წარმოადგენს ამ X_{i0}- ებისა და X_{i1} -ის სიმრავლეს აქედან გამომდინარე ყველა sig_i-სთვის მართებულია შემდეგი დებულება როცა $i = \{1, \dots K\}$ sig=($sig_1||sig_2||\dots||sig_k$)[2].

ლამპორტის ხელმოწერის სქემის გამოყენებისას მნიშვენლოვანი გავითვალისწინოთ ,რომ შეტყობინებაზე ხელმოსაწერად გვიწევს დავაგენერიროთ 2k სიგრძის მქონე ჰეშ-მნიშვნელობა როცა $M = \{0,1\}^k$,ასე რომ თუ გვინდა ჩვენი ხელომოწერა დაცული და საიმედო იყოს მოგვიწევს დავაგენერიროთ საკმაოდ გრძელი გასაღები და შესაბამისი დოკუმენტის ჰეშ-მნიშვნელობაც საკმაოდ გრძელი და კომპლექსური იქნება

მაგალითად:თუ ჩვენი ფუნქციაა $O(2^{80})$ შესაბამისი ჰეშ მნიშვნელობა იქნება მინიმუმ 160 ბიტიანი სტრიქონის სიგრძის ,ღია და გასაღებების სიგძე ერთად იქნება 160*2 ბიტი=51200 ბიტი=6400 ბაიტი აქედან გამომდინარე კი შეგვიძია დავასკვნათ,რომ ლამპორტის სქემით დაგენერირებული ღია გასაღები 50-ჯერ დიდია შესაბამისი 1024 ბიტიანი RSA-ას ღია გასაღებზე,ბუნებრივია ასეთი გრძელი და კომპლექსური ხელმოწერის გამოყენება გავლენას იქონიებს თავად პროცესის წარმადობასა და სისწრაფეზე, სწორედ ამიტომ უნდა მონახოთ გზა,რომელიც საშუალებას მოგვცემს შევამციროთ გასაღებების სიგრძე და ამავდროულად შევინარჩუნოთ ხელმოწერის დაცულობა და საიმედოობა,სწორედ ამის საშუალებას გვაძლევს ვინტერცის ხელმოწერის სქემა ,რომლის მიხედვითაც ავარჩევთ ერთ რომელიმე შემთხვევით არჩეული სტრიქონს და მისი საშუალებით სიმულაციოურად ხელს მოვაწერთ (one time signature) რამდენიმე ბიტს (n რაოდენობის ბიტს) შეტყობინების ჰეშ-მნიშვნელობიდან.დავუშვათ ვინტერცის ხელმოწერის სქემა იყენებს შეუქცევად ფუნქციას(one-way function) $f:\{0,1\}^n$->$\{0,1\}^n$ და ასევე შესაბამის ჰეშ-ფუნქციას $g:\{0,1\}^*$->$\{0,1\}^n$ ხელმოწერის წყვილის დაგენერირებისას უნდა გავითვალისწინოთ,რომ w≥2 ეს არის ბიტები ის რაოდენობა რომელსაც შემთხვევითად ვაწერთ ხელს ვინტერცის ხელმოწერის სქემის გამოყენებისას, ამ დროს t1 წარმოადგენს დროს რომელიც საჭიროს ამ ხელმოწერის შესასრულებლად, X არის თავად ხელმოწერის გასაღები ხოლო Y ვინტერცის ციფრული ხელმოწერა შესაბამისად მთელი ეს პროცესი მათემათიკური ფორმულების ენაზე აისახება შემდეგნაირად:[1] (Oorschot, 1996)*ხოლო* თავად ხელმოწერის გასაღები კი ასე გამოითვლება:$X = x_{t-1},\ldots,x_1,x_0) \in R\{0,1\}^{(n,t)}$ სადაც x_i არჩეულია შემთხვევითად ხოლო ვერსიფიკაციის გასაღები გენერირდება თითოეული x_i -სთვის შემდეგი ოპერაციბის შესრულებით $Y = y_{t-1},\ldots,y_1,y_0) \in \{0,1\}^{(n,t)}$ როცა $y_i = f^{2w-1}(x_i), \quad 0 \le i \le t-1$ გასაღების გენერირება კი მოითხოვს f ფუნქციის გამოძახებას $t(2^w-1)$-ჯერ და შესაბამისად ვერსიფიკაციის გასაღები არის $t*n$ სიგრძის[3,4].

ერთჯერადი ხელმოწერის სქემის (one-time signature scheme) ერთ-ერთ მთავარ პრობლემას წარმოადგენს ხელმოწერის გასაღებების შენხვა და მართვა. ამიტომ ციფრული ხელმოწერის გასაღებების შენახვა- გამოყენებისთვის გამოიყენება მერკლის ხე.ერთჯერადი ხელმოწერის დროს (One-time signature) ყოველ ჯერზე

გვიწევს ახალი ღია გასაღების გამოიყენება და მისი სიგრძეც არის საკმაოდ დიდი , იმისთვის რომ გავხადოთ ერთჯერადი ხელმოწერის სქემა (one-time signature) უფრო მოქნილი,სწრაფი და ეფექტური ,საჭიროა გამოვიყენოთ მერკლის ხელმოწერის სქემა ,რომელიც საშუალებას გვაძლევს ხელმოსაწერად გამოვიყენოთ ერთი ღია გასაღები მრავალ დოკუმენტზე ხელის მოსაწერად.რაიმე M შეტყობინებაზე ხელის მოწერისას ვმოქმედებთ შემდეგი თანმიმდევრობით:ჯერ ხელს ვაწერთ M შეტყობინებას ერთჯერადი ხელმოწერის სქემით და შედეგად მივიღებთ sig' ამის შემდეგ დავამატებთ კიდევ ერთ კვანძს(ფოთოლს) ბინარულ ხის შესაბამის ღია გასაღებს Y_i რომლის შესაბამისი ადგილი მერკლის ხეში იქნება $a_{0,1} = H(Y_i)$.იმისთვის რომ განვსაზღვრით გზა ჩვენ მიერ დამატებული კვანძიდან A_i მთავარ კვანძამდე უნდა დავადგინოთ იმ კვანძების შვილები(children) , რომელიც მოქცეულია ამ დიაპაზონში $A_1 \dots A_n$,თუ ჩვენ ვიცით რომ A_i არის A_{i+1} -ის შვილი მისი მნიშვნელობის გამოსათვლელად ჩვენ უნდა დავადგინოთ მისი მეზობელი კვანძი იგივე $auth_i$ რომელიც თავის მხრივ მომცემს A_{i+1} კვანძის დადგენის საშუალებას [2] (R.Merkle, 1979)(მერკლის ხეში ყოველი კვანძის დადგენა შეიძლება მისი შვილი კვანძების (leaf) კონკატენაციის ჰეშ-მნიშვნელობის გამოთვილით).ხოლო ვერსიფიკაციის დროს ხელმომწერმა იცის გასაღები რომლის საშუალებითაც ხელი უნდა მოაწეროს M შეტყობინებას $sig = (sig'||auth^0||auth^1|| \dots ||auth^{n-1})$

მერკლის ხელმოწერის სქემა ისევე როგორც ლამპორტის სქემა 30-ზე მეტი წელია რაც არსებობს ,მაგრამ მისი ოპტიმიზაციისა და კვლევის მცდელობები ბოლო ხუთი წელია რაც აქტიურად გამოჩნდა სამეცნიერო საზოგადოებებში. მერკლის ხელმოწერის სქემის მთავარ უპირატესობას წარმოადგენს ის რომ განსხვავებით სხვა ხელმოწერის სქემებისგან მისი უსაფრთხეობა და დაცულობა დამოკიდებული არ არის რაიმე მათემატიკური პრობლემის გადაწყვეტაზე ,ის დამოკიდებულია ჰეშ-ფუნქციის გაანგარიშებასა და ერთჯერადი ხელმოწერის ოპტიმიზაციაზე , იმ შემთხვევაშიც კი თუ ერთჯერადი ხელმოწერა ან ჰეშ- ფუნქცია კოლიზიამედეგი არ არის მარტივად შეიძლება მისი შეცვლა. ამ კვლევის ფარგლებში მე დავხვეწე და გავაუმჯობესე ციფრული ხელმოწერის ალგორითმი, რომელიც სტაბილურად იმუშავებს კვანტური კომპიუტერების პლატფორმაზე ,მისი საშუალებით ლამპორტის სქემის საშუელაბით ხდება ღია და დახურული გასაღებების გენერირება ხოლო შემდგომ უშუალოდ მერკლის ხელმოწერის სქემის საშუალებით ხდება ხელის მოწერა და ხელმოწერის ვერიფიცირება, მერკლის სქემის ოპტიმიზაციისას გამოვიყენე tree hash ალგორითმი , რომელმაც საშუალება მომცა მარტივად და შედარებით ნაკლებ დროში (ამ ალგორითმს ხელმოწერისთვის ესაჭიროება $2^h - 1$ ოპერაცია) ციფრულად ხელი მომეწერა დოკუმენტზე. გარდა ლამპორტის ალგორითიმისა დოკუმენტზე ხელმოსაწერად გამოვიყენე და დავაინტეგრირე ვინტერნიცის ალგორითმი,რომელმაც საშუალება მომცა სწრაფად და ეფექტურად დამეგენერირებინა ხელმოწერის გასაღებები და დამერეგულირებინა ხელმოწერისა და ვერიფიცირების დრო ,შესაბამისად უკვე მუშა ალგორითმის მრავალჯერადი გატესტვის შედეგად დავედი ქვემოთ მოცემულ შედეგებამდე(ქვემოთ მოცემული

მონაცემები ვალიდურია მხოლოდ ერთი ციფრული ხელმოწერის დაგენერირება-გამოყენებისთვის):

გენერირებისთვის საჭირო დრო	ლამპორტის ალგორითმი	ვინტერნიცის ალგორითმი	მერკლის ალგორითმი
ხელმოწერის გასაღებების გენერირებისთვის საჭირო დრო	0.0320000648499	0.0250000953674	ამ ეტაპზე არ გამოიყენება მერკლის ხე
ხელმოწერისთვის საჭირო დრო	0.0520000648499	0.0350000953684	0.0450000953674
ვერიფიცირებისთვის საჭირო დრო	0.0620000648499	0.0450000953074	0.0250000953333

REFERENCES

1 . Oorschot, P. V. (1996). *Handbook of Applied cryptography.*

2. R.Merkle. (1979). *Security,autentication and publix key systems.* Dept.of Electrial Engineering ,. Stanford univeristy.

3. 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

4. Явич М.П., Аракелян А.А. Реализация крипто-системы Merkle и ее анализ // Современные научные исследования и инновации. 2017. № 6 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2017/06/83971