Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 29-36 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

THE IDEAS OF REDUCING THE SIGNATURE SIZE IN HASH-BASED DIGITAL SIGNATURES.

ჰეშზე დაფუძნებული ელექტრონული ხელმოწერის ზომის შემცირების იდეები

Giorgi Labadze, Georgian Technical University
გიორგი ლაბაძე, საქართველოს ტექნიკური უნივერსიტეტი
Irakli Pirtskhalava Scientific Cyber Security Association
ირაკლი ფირცხალავა სამეცნიერო კიბერუსაფრთხოების ასოციაცია

ABSTRACT: The data encryption has been the traditional way of ensuring the different types of sensitive data. It is expected the massive release of quantum computers in the near future. Quantum computers can break the classical crypto schemes. Therefore the classical encryption systems have become vulnerable to quantum computer-based attacks. This involves the research efforts that look for encryption schemes that are immune to quantum computers-based attacks. This paper describes one of the few digital signature schemes, which is essentially immune to quantum computers-based attacks. These schemes have the efficiency problems. The biggest problem of this scheme is the large size of the signature. The paper offers the idea and the methodology of reducing the size of the signature size.

აბსტრაქტი: მონაცემთა დაშიფვრას აქვს ტრადიციული გზა დაიცვას სხვადასხვა სახის სენსიტიური ინფორმაცია. ახლო მომავალში მოსალოდნელია კვანტური კომპიუტერების მასიური წარმოება. კვანტურ კომპიუტერს შეუძლია გატეხოს კლასიკური კრიფტო სქემები. აქედან გამომდინარე, კლასიკური დაშიფრის სქემები შესაძლებელია გარდაიქმნას გამოუსადეგარ სქემებად კვანტური კოპიუტერით შეტევების წინააღმდეგ. ეს მოითხოვს კვლევითი მიდგომების შემუშავებას. უნდა შემუშავდეს კრიფტო სისტემები, რომელთაც ექნებათ იმუნიტეტი კვანტური კომპიუტერით შეტევების წინააღმდეგ. ეს სტატია აღწერს რამდენიმე ხელმოწერის სქემას, რომელიც შესაძლებელია მოისაზრებოდეს კვანტური კომპიუტერით შეტევის წინააღმდეგ მდგრადად. თუმცა, სქემებს აქვთ ეფექტურობის პრობლემა. სქემების ყველაზე მნიშვნელოვანი პრობლემა გახლავთ ხელმოწერის გრძელი ზომა. სტატიაში შემოთავაზებულია ხელმოწერის ზომის შემცირების იდეა და მეთოდოლოგიები.

Keywords: *hash-based, digital signatures, signature size*

საკვანძო სიტყვები: *ჰეშზე დაფუძნებული, ელექტრონული ხელმოწერები, ხელმოწერის ზომა*

1. შესავალი

მსოფლიოს წამყვანი მეცნიერები და ექსპერტები აქტიურად მუშაობენ კვანტური კომპიუტერების შექმნაზე. ახლახანს გამოქვეყნდა სტატია იმის შესახებ, რომ კორპორაცია Google-მა, NASA-მ და კოსმოსური კვლევების უნივერსიტეტების ასოციაციამ (Universities Space Research Association — USRA) ხელი მოაწერეს თანამშრომლობაზე კვანტური D-Wave პროცესორების მწარმოებელთან.

კვანტურ კომპიუტერს ექნება შესაძლებლობა დაანგრიოს უმეტესი წილი ან აბსოლუტურად ყველა ტრადიციული კრიპტოსისტემა, რომელიც ფართოდ გამოყენებადია პრაქტიკაში და კონკრეტულად მთელი რიცხვების ფაქტორიზაციის ამოცანაზეა დაფუძნებული (მაგალითად RSA). ზოგიერთი კრიპტოგრაფიული სისტემა, როგორიც გახლავთ RSA - ოთხი ათას ბიტიანი გასაღებით, უსაფრთხოდ ითვლება დიდი კლასიკური კომპიუტერების თავდასხმებისგან, მაგრამ უძლურია დიდი კვანტური კომპიუტერების თავდასხმების საწინააღმდეგოდ. კრიპტოსისტემა RSA გამოიყენება სხვადასხვა პროდუქტებში, განსხვავებულ პლატფორმებზე მრავალ დარგში. დღესდღეობით RSA კრიპტოსისტემა ინერგება ბევრ კომერციულ პროდუქტში, რომელთა რაოდენობაც მუდმივად იზრდება. აგრეთვე იგი გამოიყენება Microsoft-ის, Apple-ის, Sun-ის და Novell-ის ოპერაციულ სისტემებში. აპარატულ შესრულებაში RSA ალგორითმი გამოიყენება დაცულ ტელეფონებში, Ethernet ქსელურ პლატებში, სმარტ ბარათებში, და ფართოდ გამოიყენება კრიპტოგრაფიულ აპარატულ უზრუნველყოფაში. ამასთან ერთად, ალგორითმი არის Internet დაცული კომუნიკაციების ძირითადი პროტოკოლების ნაწილი, მათ შორის S/MIME, SSL და S/WAN, და აგრეთვე გამოიყენება მრავალ დაწესებულებაში, მაგალითად სამთავრობო ორგანიზაციებში, ბანკებში, კორპორაციების უმრავლესობაში, სახელმწიფო ლაბორატორიებსა და უნივერსიტეტებში [1-4].

შემუშავებულია RSA-ს სხვადასხვა „კვანტური თავდასხმებისადმი მდგრადი“ ალტერნატივები. დღესდღეობით ამ სისტემებზე ფიქსირდება ეფექტური თავდასხმების მთელი რიგი.

აღსანიშნავია ეფექტურობის ასპექტის მნიშვნელობა. დღესდღეობით ექსპერტებმა კრიპტო ალგორითმების შესრულების სისწრაფეში საკმაოდ კარგ შედეგებს მიაღწიეს. კვლევის შედეგად ცნობილი ხდება, რომ შემოთავაზებული პოსტ-კვანტური კრიპტო სისტემები შედარებით ნაკლებ ეფექტურია, რადგან მათი რეალიზაციის ალგორითმები მოითხოვს ბევრად მეტ დროს შესრულების და ვერიფიკაციისთვის.

2. ციფრული ხელმოწერები

ციფრული ხელმოწერა გახდა მნშვნელოვანი ტექნოლოგია ინტერნეტისა და სხვა IT-ინფრასტრუქტურის უსაფრთხოებაში. ციფრული ხელმოწერა უზრუნველყოფს

ავთენტურობას, მთლიანობას და მონაცემის იდენთიფიცირებას. ციფრული ხელმოწერა ფართოდ გამოიყენება იდენთიფიცირების და ავთენთიფიკაციის პროტოკოლებში. ამგვარად, არსებული უსაფრთხო ციფრული ხელმოწერის ალგორითმს აქვს გადამწყვეტი მნიშვნელობა IT უსაფრთხოების მხარდაჭერისათვის.

ციფრული ხელმოწერის ალგორითმები, რომლებიც დღეს პრაქტიკაში გამოიყენება გახლავთ RSA, DSA, ECDSA. თუმცა ისინი არ არიან კვანტურად მდგრადები , რადგან მათი უსაფრთხოება დამყარებულია რთულ ფაქტორიზაციაზე, დიდ შედგენილ მთელ რიცხვებზე და დისკრეტული ლოგარითმების გამოთვლაზე.

ჰეშზე დამყარებული ციფრული ხელმოწერის სქემები, რომელსაც წარმოვადგენთ, გვთავაზობს ძალიან საინტერესო ალტერნატივებს . როგორც სხვა ციფრული ხელმოწერის სქემა, ასევე ჰეშზე დამყარებული ციფრული ხელოწერის სქემა იყენებს კრიფტოგრაფიულ ჰეშ ფუნქციას.

3. ერთჯერადი ხელმოწერის სქემები.

ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემა (LD-OTS) წარმოადგენს:

დავუშვათ n არის დადებითი მთელი რიცხვი, უსაფრთხოების პარამეტრი

ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემაში [5].

ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემა იყენებს ცალმხირვ ფუნქციას.

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

და კრიფტოგრაფიული ჰეშ ფუნქციას.

$$g :\{0.1\}^{*}\rightarrow\{0,1\}n$$

LD-OTS გასაღებების წყვილების გენერაცია. ხელმოწერის გასაღებია X ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემიდან შედგება 2n ბიტიანი n სიგრძის სტრიქონებისგან, რომელიც აირჩევა თანაბრად, შემთხვევითობის მეთოდით.

$$X = (x_{n-1}[0], x_{n-1}[1],\ldots,x_1[0], x_1[1], x_0[0], x_0[1]) \in R \{0,1\}(n.2n). \quad (1)$$

LD-OTS ვერიფიკაციის გასაღები Y

$$Y = (y_{n-1}[0], y_{n-1}[1],\ldots,y_1[0], y_1[1], y_0[0], y_0[1]) \in R \{0,1\}(n.2n). \quad (2)$$

სადაც

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

ანუ LD-OTS გასაღების გენერაცია მოითხოვს 2n შეფასებას F- იდან.

სტრიქონი და ვერიფიკაციის გასაღები არის 2n ბიტიანი n სიგრძის სტრიქონები.

LD-OTS ხელმოწერის გენერაცია. A დოკუმენტი $M \in \{0,1\}(n,n)$.

ხემოწერისთვის იყენებს ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემას (LD-OTS) ხელმოწერის გასაღებით X, (1) გამოსახულების მნიშვნელობით.

დავუშვათ $g(M)=d = (d_{n-1},...,d_0)$ არის შეტყობინების წარმოდგენა M იდან. შემდეგ LD-OTS ხელმოწერა არის

$$\sigma = (x_{n-1}[d_{n-1}],\ldots,x_1[d_1]x_0[d_0] \in \{0,1\}(n,n) \qquad (4)$$

ეს ხელმოწერა წარმოადგენს n ბიტ სტრიქონების თანმიმდევრობას , რომელთაგან თითეულის სიგრძეა n. შემდეგ არჩეულია ფუნქცია, რომლის შეტყობინებასაც წარმოადგენს d-ს. ბიტური სტრიქონი ამ ხელმოწრაში არის x_i [0], თუ i ბიტ d ში ტოლია 0-ის, ხოლო ყველა სხვა შემთხვევაში არის x_i [1] . ხელმოწერა არ მოითხოვს შეფასებას f-იდან. ხელმოწერის სიგრძეა 2n.

LD-OTS ვერიფიკაცია. ხელმოწერის ვერიფიკაციისთვის $\sigma = (\sigma_{n-1},\ldots, \sigma_0)$. M დან, როგორც გამოსახულება (4) ში, ვერიფიკაცია ითვლის შეტყობინების წარდგენას $d= (d_{n-1},\ldots, d_0)$ შემდეგ ის ამოწმებს

$$(f(\sigma_{n-1}),\ldots, f(\sigma_0))=(y_{n-1}[d_{n-1}],\ldots, y_0[d_0]). \qquad (5)$$

ხელმოწერის ზომა გახლავთ n^2 .

მიუხედავად იმისა, რომ გასაღების და ხელმოწერის გენერაცია LD-OTS ეფექტურია, ხელმოწერის ზომა საკმაოდ დიდია. ვინტერნიცის ერთჯერადი ხელმოწერის სქემაში OTS (W-OTS) ხელმოწერის ზომა მნიშვნელოვნად პატარაა. იდეა მდგომარეობს იმაში, რომ გამოვიყენოთ ერთი სტრიქონი ერთჯერადი ხელმოწერის გასაღებში, რამდენიმე ბიტის ერთდროული ხელმოწერისთვის დაჰეშილ შეტყობინებაში. მეთოდი შემოთავაზებული იქნა მერკლეს მიერ 1979 წელს [6].

4 . მერკლეს ხის იდენთიფიკაციის სქემა

ერთჯერადი ხელმოწერის სქემები, შემოთავაზებული ბოლო ვერსიით, არ არიან გამოყენებადი პრაკტიკული სიტუაციების უმრავლესობისთვის, რადგან ყოველი გასაღების წყვილი გამოიყენება მხოლოდ ერთი ხელმოწერისთვის . 1979 წელს რალფ მერკლემ შემოგვთავაზა ამ პრობლემის გადაწყვეტა. მისი იდეა მდგომარეობს შემდეგში, რომ გამოვიყენოთ სრული ბინარული ჰეშ ხე,იმისათვის რომ შევამციროთ ვერიფიკაციის გასაღების რაოდენობა, ანუ შევცვალოთ კონკრეტული ფიქსირებული გასაღებების რაოდენობა ერთით, რომლსაც წარმოადგენს ხის ფესვი.

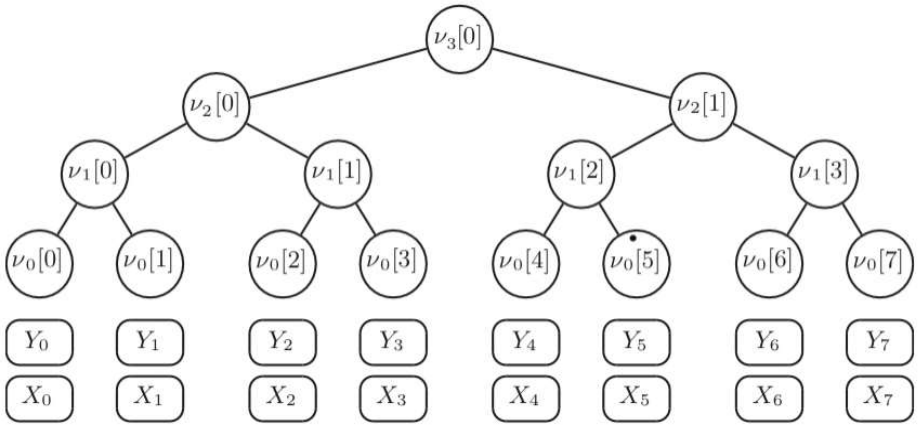
მერკლეს ხელმოწერის სქემა (MSS) მუშაობს ნებისმერ კრიპტოგრაფიულ ჰეშ ფუნქციასთან და ნებისმიერ ერთჯერად ხელმოწერის სქემასთან . განმარტებისთვის დავუშვათ $g: \{0,1\}^* \to \{0,1\}^n$ არის კრიპტოგრაფიული ჰეშ ფუნქცია. ჩვენ ასევე ვთვლით, რომ შეირჩა ერთჯერადი ხელმოწერის სქემა [7].

4.1. MSS გასაღებების წყვილის გენერაცია

ხელმომწერი ირჩევს $H \in N, H \geq 2$. შემდეგ დაგენერირებული გასაღებების წყვილი შეძლებს დოკუმენტების 2^H ხელმოწერა/ვერიფიკაციას. აღსანიშნავია, რომ არის მნიშვნელოვანი განსხვავება ისეთ ხელმოწერის სქემებთან, როგორიც არის RSA და ECDSA, სადაც პოტენციური, შემთხვევითი და ბევრი დოკუმენტები შეიძლება ხელმოწერილ/ ვერიფიცირებული იქნას ერთი წყვილი გასაღებით. თუმცა , ეს განსაზღვრული რიცხვი ასევე შეზღუდულია მოწყობილობით, რომელიც გენერირდება ხელმოწერით ან რაიმე პოლისით. ხელმომწერი აგენერირებს 2^H ერთჯერად გასაღებების წყვილს $(X_j, Y_i), 0 \leq j < 2^H$. ხის შიდა კვანძები მერკლეს ხეში გამოითვლება შემდეგი წესის მიხედვით: მშობელი კვანძი არის ჰეშ მნიშვნელობა, კონკატენცია მისი მარცხენა და მარჯვენა შვილების. MSS ღია გასაღების წყვილი არის მერკლეს ხის ფესვი. MSS საიდუმლო გასაღები წარმოადგენს 2^H ერთჯერადი გასაღებების მიმდევრობას. რომ ვიყოთ უფრო ზუსტი, მერკლეს ხეში აღვნიშნოთ კვანძები

$$\nu_h[j] = g(\nu_{h-1}[2j] || \nu_{h-1}[2j+1]), 1 \leq h \leq H, 0 \leq j < 2^{H-h}. \quad (6)$$

მაგალითი მოცემულია $H = 3$.



ნახაზი 1 მერკლეს ხე სიმაღლე $H = 3$

MSS გასაღებების წყვილების გენერაცია მოითხოვს გამოთვლებს 2^H ერთჯერადი გასაღებების წყვილიდან და $2^{H+1} - 1$ შედარების ჰეშ ფუნქციას.

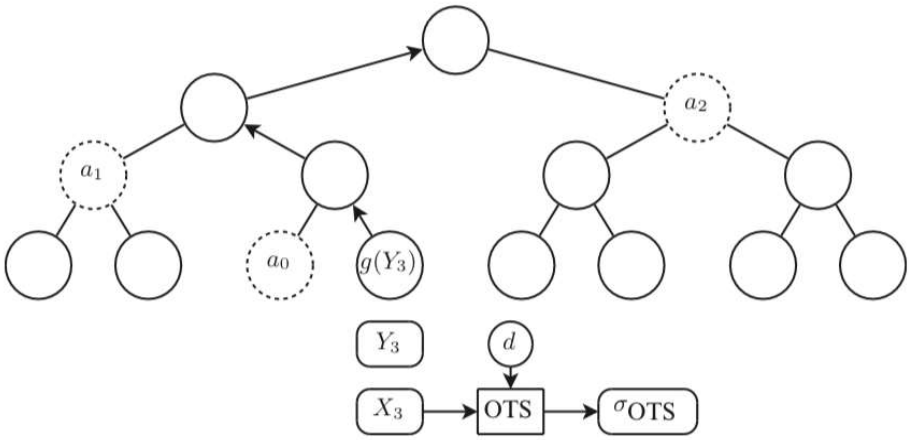
4.2 MSS ხელმოწერის გენერაცია

MSS თანმიმდევრულად იყენებს ერთჯერადი ხელმოწერის გასაღებს, რომ დააგენერიროს ხელმოწერა . შეტყობინება M-ის ხელმოსაწერად, ხელმომწერი პირი თავიდან ითვლის n-ბიტ ჰეშს, $d = g(M)$, შემდეგ აგენერირებს ჰეშ ერთჯერად ხელმოწერას σ_{OTS} , sth გამოყენებით , ერთჯერადი ხელმოწერის გასაღები არის $X_s, s \in \{0, \dots, 2^H - 1\}$. მერკლეს ხელმოწერა მოიცავს აღნიშნულ ერთჯერად ხელმოწერას და კორესპონდენციის ერთჯერად ვერიფიკაციას Y_s. რომ დავმტკიცოთ Y_s ვერიფიკაციის ავთენტურობა ,ხელმომწერი ასევე რთავს ინდექსს s , ასევე ავთენტიფიკაციის გზა ვერიფიკაციის გასაღები Y_s თვის. მერკლეს ხეში ბოლოების თანმიმდევრობაა $A_s = (a_0, \dots., a_{H-1})$. ეს ავთენთიფიკაციის ინდექსების გზა საშუალებას აძლევს ვერიფიკატორს აშენდეს უმოკლესი გზა ხის ბოლოდან მის ფესვამდე. ბოლო h აუთენთფიკაციის გზაში წარმოადგენს მშობელ დაბოლოებას. სიმაღლით h გზა მერკლეს ხეში ბოლოდან არის $g(Y_s)$ ფესვამდე :

$$a_h = \begin{cases} v_h\,[s/2^h - 1], if \lfloor s/2^h \rfloor \equiv 1\ mod\ 2 \\ v_h\,[s/2^h - 1], if \lfloor s/2^h \rfloor \equiv 0\ mod\ 2 \end{cases} \quad (7)$$

$$for\ h = 0, \dots H - 1.$$

$$\sigma_s = (s, \sigma_{OTS,} Y_s, (a_0, \dots., a_{H-1})) \quad (8)$$



ნახაზი №3 მერკლეს ხელმოწერის გენერაცია $s = 3$. მონიშული ბოლოები ასახავს ავთენთიფიკაციის გზას დაბოლოებამდე $g(Y_3)$. ისრები გვაჩვენებენ გზას ბოლოდან $g(Y_3)$ ფესვამდე .

4.3 MSS ხემოწერის ვერიფიკაცია

მერკლეს ხის ხელმოწერის ვერიფიკაცია მოიცავს ორ ეტაპს. პირველ ეტაპზე ვერიფიკატორი იყენებს ერთჯერად ვარიფიკაციის გასაღებს Y_s -ს და ერთჯერად ხელმოწერას σ_{OTS}-ს. ვერიფიკაციისთვის d-ს გამოთვლა ხდება შემოწმების ალგორითმის დახმარებით, რომელიც შესაბამისია ერთჯერადი ხელმოწერის სქემის. მეორე ეტაპზე ვერიფიკატორი ამოწმებს ვერიფიკაციის ერთჯერადი გასაღების შესაბამისობას Y_s -თან მარტივი გზით $(p_0, \dots, p_H)$, sth $g(Y_s)$ დაბოლოებიდან მერკლეს ხის ფესვამდე. ის იყენებს ინდექსს s აუთენთიფიკაციის გზისთვის $(a_0, \dots., a_{H-1})$ და გამოიყენება შემდეგი კონსრტუქცია.

$$p_h = \begin{cases} g(a_{h-1} \| p_{h-1}), if \lfloor s/2^h \rfloor \equiv 1 \ mod\ 2 \\ g(p_{h-1} \| a_{h-1}), if \lfloor s/2^h \rfloor \equiv 0 \ mod\ 2 \end{cases} \qquad (19)$$

$$for\ h = 1, \dots. H \qquad p_0 = g(Y_s).$$

ინდექსი s გამოიყენება იმისთვის, რომ დავადგინოთ თანრიგი და ავთენთიფიკაციის გზის კვანძები. კვანძები, რომლებიც ბოლოდან $g(Y_s)$ მერკლეს ფესვამდე უნდა გაერთიანდნენ. Y_s წარმატებულია, თუ p_H ტოლია ღია გასაღების.

5 ხელმოწერის შემცირების იდეა

როგორც (8) ფორმულაში აღინიშნა, მერკლეს სქემაში ხელმოწერა არის $\sigma_s = (s, \sigma_{OTS,} Y_s, (a_0, \dots., a_{H-1}))$. ეს ხელმოწერა შეიცავს $\sigma_{OTS,}$ - ერთჯერად ხელმოწერას. როგორც ვხედავთ, მერკლეს ხელმოწერაში, ხელმოწერის ზომა საკმაოდ მეტია, ვიდრე ერთჯერადი ხემოწერის დროს. ჩვენი მიზანია შევამციროთ ხელმოწერის ზომა.

აღსანიშნავია, რომ ბოლოს შემოთავაზებული ერთჯერადი ხელმოწერის სქემა არ არის გამოყენებადი პრაკტიკული სიტუაციების უმრავლესობისთვის, რადგან ყოველი გასაღების წყვილი გამოიყენება მხოლოდ ერთი ხელმოწერისთვის. უნიკალური გასაღების გადაცემა თითოეული ხელმოწერისთვის დღევანდელ პირობებში არარეალურია. კვანტური კომპიუტერები კი მოგვცემენ საშუალებას გადავცეთ გასაღებები ეფექტურად და უსაფრთხოდ [8]. შესაბამისად, მიზანშეწონილია კვანტური გასაღების პროტოკოლის

ინტეგრაცია ერთჯერად ხელმოწერის სქემაში და მისი ოპტიმიზაცია. აღსანიშნავია, რომ ვინტერნიცის მიერ შემოთავაზებულ ხელმოწერის სქემაში, ხელმოწერის ზომა ნაკლებია ვიდრე ლამპორტის სქემაში. საინტერესო იქნებოდა ამ სქემაში ზემოთ აღნიშნული პროტოკოლის ინტეგრაცია.

ბიბლიოგრაფია

1. Gagnidze A., Iavich M., Iashvili G., (2017) Analysis of post quantum cryptography use in practice. Bulletin of the Georgian National Academy of Sciences, 2, 12: 29-36
2. Gagnidze, A., Iavich, M., Iashvili, G., Novel version of merkle cryptosystem, Bulletin of the Georgian National Academy of Sciences, 2017
3. Iavich, M., Gagnidze, A., Iashvili, G., Hash based digital signature scheme with integrated TRNG, CEUR Workshop Proceedings, 2018
4. Paquin C., Stebila D., Tamvada G. (2020) Benchmarking Post-quantum Cryptography in TLS. In: Ding J., Tillich JP. (eds) Post-Quantum Cryptography. PQCrypto 2020. Lecture Notes in Computer Science, vol 12100. Springer, Cham. https://doi.org/10.1007/978-3-030-44223-1_5
5. Ajtai, M. (1986) Generating hard instances of lattice problems. In Complexity of computations and proofs, volume 13 of Quad. Mat., pp. 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
6. Buchmann J., Dahmen E., Ereth S., Hülsing A., Rückert M. (2011) On the Security of the Winternitz One-Time Signature Scheme In: Nitaj A., Pointcheval D. (eds) Progress in Cryptology – AFRICACRYPT 2011. Lecture Notes in Computer Science, vol 6737. Springer, Berlin, Heidelberg
7. R. Merkle. (1979) Secrecy, authentication and public key systems / A certified digital signature Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University.
8. Hu Z., Gnatyuk S., Okhrimenko T., Tynymbayev S. and Iavich M. High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security, Issue 12 (3), pp. 1-10, 2020