საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

გიორგი ლაბაძე

კვანტური და პოსტ-კვანტური კრიფტოგრაფია

სადოქტორო პროგრამა: ინფორმატიკა

შიფრი: 0613

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

თბილისი

2021 წელი

სამუშაო შესრულებულია საქართველოს ტექნიკური უნივერსიტეტში
ინფორმატიკისა და მართვის სისტემების ფაკულტეტი
გამოთვლითი მათემატიკის დეპარტამენტი

ხელმძღვანელი: პროფესორი **მაქსიმ იავიჩი**

რეცენზენტები: _____

დაცვა შედგება 2021 წლის „-------„ „----------„ „--------„ საათზე საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკის, მართვის და ხელსაწყოთმშენებლობის საუნივერსიტეტო სადისერტაციო საბჭოს სხდომაზე, კორპუსი ----------, აუდიტორია ----------
მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ის ბიბლიოთეკაში,
ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

საუნივერსიტეტო სადისერტაციო საბჭოს
სწავლული მდივანი, პროფესორი თ. კაიშაური

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

D-Wave 2X - უახლესი კვანტური პროცესორია, რომელიც შეიცავს 2048 ფიზიკურ კუბიტს (კვანტური განმუხტვები, ინფორმაციის შენახვის უმცირესი ერთეულები კვანტურ კომპიუტერში). 1152 კუბიტი კვანტური კომპიუტერის ამ მოდელში გამოიყენება გამოთვლების შესასრულებლად. თითოეული დამატებითი კუბიტი ორჯერ ზრდის ძიების სივრცეს, შესაბამისად იზრდება გამოთვლების სიჩქარეც.

ზემოთ აღნიშნულიდან გამომდინარე, კვანტურ კომპიუტერს ექნება შესაძლებლობა დაანგრიოს უმეტესი წილი ან აბსოლუტურად ყველა ტრადიციული კრიპტოსისტემები, რომლებიც ფართოდ გამოყენებადია პრაქტიკაში და კონკრეტულად მთელი რიცხვების ფაქტორიზაციის ამოცანაზე დაფუძნებული სისტემები (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 კრიპტოგრაფიულ აპარატულ უზრუნველყოფაში. ამასთან ერთად, ალგორითმი არის Internet დაცული

კომუნიკაციების ძირითადი პროტოკოლების ნაწილი, მათ შორის S/MIME, SSL და S/WAN, აგრეთვე გამოიყენება მრავალ დაწესებულებაში, მაგალითად სამთავრობო ორგანიზაციებში, ბანკებში, კორპორაციების უმრავლესობაში, სახელმწიფო ლაბორატორიებსა და უნივერსიტეტებში.

RSA BSAFE დაშიფრვის ტექნოლოგია გამოიყენება დაახლოებით 500 მილიონი მომხმარებლის მიერ მთელ მსოფლიოში. რადგან ხშირ შემთხვევაში ამ დაშიფრვის ტექნოლოგიებში გამოიყენება RSA ალგორითმი, იგი შეიძლება ჩაითვალოს მსოფლიოში საერთო (public) გასაღების ერთ-ერთ გავრცელებულ კრიპტოსისტემად, რასაც აშკარად გააჩნია ზრდის ტენდენცია Internet-ის ზრდასთან ერთად. აქედან გამომდინარე RSA-ს დანგრევა ბევრ დარგში გამოიწვევს პროდუქტების უმეტესობის გატეხვას, რაც შესაძლოა სრულ მარცხად იქცეს.

მეცნიერული სიახლე. სადისერტაციო ნაშრომის მეცნიერული სიახლეს წარმოადგენს ახალი პოსტ-კვატური კრიპტოსისტემა. შექმნილი ახალი სქემის დიდი უპირატესობა, უკვე არსებულ სხვა სქემებთან შედარებით განაპირობა ჰიბრიდულმა მიდგომამ, პოსტ-კვანტური გასაღების გადაცემის შემთხვევაში ჩვენ უსაფრთხოების მისაღწევად გვჭიდება მერკლის ხის იდენთიფიკაციის სქემა, რადგან პრაკტიკული სიტუაციების უმრავლესობისთვის ყოველ ჯერზე უიკალური გასაღების გადაცემა შეუძლებლია. ამიტომ მერკლის იდეა ხის ფესივს ალგორითმით უსაფრთხოების შენარჩუნება ხერხდება თუმცა მისი ზომა არის დიდი და ინფორმაციის მიმოცვლის ზრდასთან ერთად იქმნება გადაუჭრელი ეფექტურობის პრობლემა.

აქედან გამომდინარე, მოძიებული იქნა მიდგომა რომლის საშვალებითაც შესაძლებელი იქნებოდა უნიკალური გასაღების გადაცემა და გასაღების სიგრძე მაქსიმალურად მიახლოებული იქნებოდა შენონის აბსოლიტური უსაფრთხოების მოთხოვნასთან. კლასიკურ აუთენთიფიცირებულ არხთან ერთად შეირჩა კვანტური გადაცემის არხი სადაც ინფორმაციის კოდირება და გადაცემა ხდება უმცირესი ნაწილაკების საშუალებით დღეს-დღეობით

საუკეთესოდ ამ ამოცანის შესასრულებლად ითვლება ფოტონები. პროტოკოლი რომლის მიხედვითაც კვანტურ არხში ვახდენთ გასაღების გადაცემას არის BB84 მას პრივილეგირებული ადგილი უკავია არსებულ პროტოკოლთა სიაში: ეს ის არის, რომელსაც ყველაზე მეტად აანალიზებენ და ყველაზე ხშირად ანხორციელებენ, მათ შორის მათ, რომელიც კომერციულ პროდუქტებში გამოიყენება. კიდევ ერთი გამოკვეთილი უპირატესობა რაც BB84 გამყენებამ მოგვცა არის ის რომ ნებიმერი სახის მოსმენა კანონიერი მხარეებისთვის იქნება შესამჩნევი და შემდეგ ტენკურად ამ ფაქტის გამოსწორება შესაძლებელია. რანდგან ჩვენ მოვხსენით გსაღებების სტრიმის გადაცემის პრობლემა.

პოსტ კვანტურში დაგვრჩა ხელმოწერის ეფექტურობის გაუჯობესების საკითხი.

შესწავლილი იქნა ჰეშზე დაფუძნებული ხელმოწერის სქემები, რომელნიც კიდევ ერთხელ ხაზგასმით უნდა აღინიშნოს მდგრადები არან პოსტ კვანტურ ეპოქაში

და შერჩეულუ იქნა ვინტერნიცის ერთჯერადი ხელმოწერის სქემა. მოხდა გასაღებების წყვილების გენერაცია, ხელმოწერის გენერაცია და ვერიფიკაცია. გამოიკვეთა რომ არა მარტო მერკლესთან არამედ სხვა უსაფრთხო სქემებთან შედარებით მისი ზომა მნიშვნელოვნად პატარაა. ვინტერნიცის და BB84 გაერთიანებამ შექმნა ჰიბრიდული, ეფექტური და უსაფრთხო სისტემა.

კვლევის მიზანი. 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, მათი რეალიზაციის ალგორითმები მოითხოვს ბევრად მეტ დროს მათი შესრულების და ვერიფიკაციისთვის.

არაეფექტური კრიპტოგრაფია შეიძლება იყოს მისაღები უბრალო მომხმარებლებისთვის, მაგრამ ვერ იქნება მისაღები ინტერნეტის სერვერებისთვის, რომლებიც წამში ათასობით კლიენტს ამუშავებენ. Google-ს დღესდღეობით გააჩნია პრობლემები მიმდინარე კრიპტოგრაფიასთან, არ არის რთული წარმოსადგენი რა მოხდება როდესაც კრიპტო ალგორითმების შესრულებას უფრო მეტი დრო დასჭირდება.

თანამედროვე კრიპტოსისტემის განვითარებას და გაუმჯობესებას მრავალი წელი დასჭირდა. ამასთან ერთად, მათზე ყოველთვის ფიქსირდებოდა თავდასხმები. როდესაც ისაზღვრება დაშიფრვის უსაფრთხო ფუნქცია და იგი სტანდარტად იქცევა, მას ესაჭიროება შესაბამისი პროგრამული და ხშირ შემთხვევაში აპარატული უზრუნველყოფის რეალიზაცია.

აქედან გამომდინარე კვლევის მიზანია შეიქმნას ახალი კრიფტოსისტემა. ეს კრიფტოსისტემა უნდა იყოს მდგრადი კვანტური კოპიუტერებით შეტევების მიმართ. აგრეთვე ეს კრიფტოსისტემა უნდა იყოს უსაფრთხო და ეფექტური.

კვლევის ობიექტი და მეთოდები. კვლევის ობიექტი არის არსებული RSA ალტერნატივების ანალიზი. აგრეთვე კვლევის ობიექტი არის კვანტური გასაღების გადაცემის ალგორითმების ანალიზი.

კრიპტოგრაფიული სქემების რეალიზაციის დროს უნდა იყოს უზრუნველყოფილი არა მხოლოდ ფუნქციის მუშაობის გამართულობა და მისი ეფექტური სიჩქარე, არამედ სხვადასხვა ტიპის გაჟონვების თავიდან აცილება. ახლახანს დაფიქსირდა RSA და AES რეალიზაციებზე წარმატებული «cache-timing» შეტევები, რის შემდეგაც კომპანია Intel-მა დაამატა AES ინსტრუქციები თავის პროცესორებში.

როგორც ვხედავთ, უსაფრთხო და ეფექტური პოსტ-კვანტური კრიპტო სისტემების შექმნისთვის და რეალიზაციისთვის საკმაოდ დიდი მოცულობის სამუშაოები არის ჩასატარებელი.

ციფრული ხელმოწერა გახდა მნშვნელოვანი ტექნოლოგია ინტერნეტისა და სხვა IT-ინფრასტრუქტურის უსაფრთხოებაში. ციფრული ხელმოწერა, უზრუნველყობს ავთენტურობას, მთლიანობას და მონაცემის იდენთიფიცირებას. ციფრული ხელოწერა ფართოდ გამოიყენება იდენთიფიცირების და აუთენთიფიკაციის პროტოკოლებში. ამგვარად არსებული უსაფრთხო ციფრული ხელმოწერის ალგორითმს აქვს გადამწყვეტი მნიშვნელობა IT უსაფრთხოების მხარდაჭერისთვის.

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

ჰეშზე დამყარებული ციფრული ხელმოწერის სქემები, რომლებსაც წარმოვადგენთ, გვთავაზობს ძალიან საინტერესო ალტერნატივებს. როგორც სხვა ციფრული ხელმოწერის სქემა, ასევე ჰეშზე დამყარებული ციფრული ხელოწერის სქემა იყენებს კრიფტოგრაფიულ ჰეშ ფუნქციას. მათი უსაფრთხოება დამოკიდებულია ჰეშ ფუნქციით წინაღმდეგობრივი შეჯახებით. რეალურად ჩვენ წარმოვადგენთ ჰეშზე დამყარებულ ციფრულ ხელმოწერის სქემას, რომელიც არის უსაფრთხო, მაშინ და მხოლოდ მაშინ, როდესაც ჰეშ ფუნქციის საფუძველი არის მდგრადი წინაღმდეგობების მიმართ. არსებობა შეჯახებასთან მდგრადი ჰეშ-ფუნქციის, შეიძლება დავინახოთ როგორც მინიმალური მოთხოვნა ციფრული ხელმოწერის სქემის არსებობისთვის, რომელსაც შეუძლია მონიშნოს (მოაწეროს) ბევრი დოკუნემტი ერთი პირადი გასაღებით. ხელმოწერის ეს სქემა ნიშნავს დოკუმენტების (თვითნებური ბიტების გრძელი მასივი) ციფრულ ხელმოწერას (ბიტების მასივი ფიქსირებული სიგრძით). ეს გვაჩვენებს, რომ ციფრული ხელმოწერა სინამდვილეში გახლავთ ჰეშ ფუნქცია. ეს ჰეშ ფუნქციები უნდა იყოს წინააღმდეგობის მიმართ მდგრადი: თუ შესაძლებელია შეიქმნას ორი დოკუმენტი ერთი და იგივე ციფრული

ხელმოწერით, ხელმოწერის სქემა აღარ შეიძლება ჩაითვალოს უსფრთხოდ. ეს არგუმენტი გვანახებს, რომ არსებობს ციფრული ხელმოწერის სქემა დამყარებული ჰეშზე, რამდენადაც არსებობს ნებისმიერი ციფრული ხელმოწერის სქემა, რომლსაც შეუძლია ხელი მოაწეროს რამოდენიმე დოკუმენტს ერთი გასაღების გამოყენებით. შედეგდ ჰეშზე დამყარებული ხელმოწერა არის მნიშვნელოვანი კანდიდატი პოსტ-კვანტური ხელმოწერისთვის. თუმცა დამტკიცებული არ არის მათი მდგრადობა კვანტური კომპიუტერის პირობებში, მოთხოვნები მათი უსაფრთხოების მიმართ არის მინიმალური. მიხედავად იმისა, რომ ყოველი ახალი კრიფტოგრაფიული სქემა გვაძლევს ხელმოწერის ახალ სქემას. ასე რომ, უსაფრთხო სქემების შექმნა დამოუკიდებელია რთულ ალგორითმებზე რიცხვთა თეორიიდან და ალგებრიდან. აკმაყოფილებს კონსტრუცქიები სიმეტრიული კრიფტოგრაფიიდან.

ეს არის კიდევ ერთ დიდი უპირატესობა ჰეშზე დამყარებული ხელმოწერის სქემის. აღწერილი ჰეშ ფუნცქია შეიძლება არჩეული იქნას, აპარატურული, პროგრამული რესურსების გათვალიწინებით. მაგალითად, ხელმოწერის სქემა რიალიზებული უნდა იქნას ჩიპზე, რომელიზეც უკვე რიალიზებულია AES. ჰეშ ფუნქცია დამყარებული AES შესაძლებელია გამოყენებული იქნას იმავე ხემოწერის სქემის ზომის შესამცირებლად და მისი შესრულების დროის ოპტიმიზაციისთვის. ციფრული ხელმოწერის სქემა დამყარებული ჰეშ ფუნქციაზე, შექმნილი რალფ მერკლის მიერ, მერკლემ დაიწყო ერჯერადი ხელმოწერის სქემით, ისეთით როგორიცაა: ლამპორტი და დიფი. ერთჯერადი ხელმოწერა არის მეტად ფუნდამენტალური. ერთჯერადი ხელმოწერის უსაფრთხო სქემები ითხოვენ მხოლოდ ცალმხრივ ფუნქციას. როგოც გვანახებს როპელი, ცალმხრივი ფუნქცია არის აუცილებელი და საკმარისი უსაფრთხო ციფრული ხელმოწერისთვის. ასე რომ, ერთჯერადი ხემლოწერის სქემები ნამდვილად წარმოადგენს ფუნდამენტალურ ტიპს ციფრული ხელმოწერის სქემებში. მიუხედავად ამისა მათ აქვთ სეროზული უკმარისობანი. გასაღებების ერთი

წყვილი, შემდგარი ხემლოწერის საიდუმლო გასაღებისგან და ღია გასაღებისგან შესაძლებელია გამოყენებული იქნას მხოლოდ ერთი დოკუმენტის შემოწმებისთვის. ეს არ არის საკმარისი აპლიკაციების უმრავლესობისთვის. ეს იყო მერკლის იდეა გამოეყენებინა ჰეშ ხე, რომელიც ამცირებს ბევრი ერთჯერადი გასაღებების ვალიდურობას (ჰეშ-ხის ფოთლები) და ნამდივლობას ერთი ღია გასაღების (ჰეშ ხის ფესვი). მერკლეს პირველადი კონსტრუქცია არ იყო საკმარისად ეფექტური, ძირითადად RSA ხელმოწერის სქემასთან შედარებით. თუმცა მას შემდეგ მოძიებული იქნა ბევრი გაუმჯობესება და ხელმოწერის მიდგომა დამყარ ებული ჰეშზე, არის მეტად წარმატებული ალტერნატივა RSA და ელიფსური მრუდის ხემოწერის სქემების .

კვლევის ძირითადი შედეგები. სადოქტორო კვლევის ფარგლებში შემუშავდა ახალი კრიფტოგრაფიული ჰიბრიდული სქემა, პოსტ-კვანტური გასაღების გადაცემის შემთხვევაში ჩვენ უსაფრთხოების მისაღწევად გვჭიდება მერკლის ხის იდენთიფიკაციის სქემა, რადგან პრაკტიკული სიტუაციების უმრავლესობისთვის ყოველ ჯერზე უნიკალური გასაღების გადაცემა შეუძლებლია. ამიტომ, მერკლის იდეა ხის ფესვის ალგორითმით უსაფრთხოების შენარჩუნება ხერხდება, თუმცა მისი ზომა არის დიდი და ინფორმაციის მიმოცვლის ზრდასთან ერთად იქმნება გადაუჭრელი ეფექტურობის პრობლემა.

აქედან გამომდინარე, მოძიებული იქნა მიდგომა, რომლის საშუალებითაც შესაძლებელი იქნებოდა უნიკალური გასაღების გადაცემა და გასაღების სიგრძე მაქსიმალურად მიახლოებული იქნებოდა შენონის აბსოლიტური უსაფრთხოების მოთხოვნასთან. კლასიკურ აუთენთიფიცირებულ არხთან ერთად შეირჩა კვანტური გადაცემის არხი, სადაც ინფორმაციის კოდირება და გადაცემა ხდება უმცირესი ნაწილაკების საშუალებით. დღეს-დღეობით საუკეთესოდ ამ ამოცანის შესასრულებლად ითვლება ფოტონები. პროტოკოლი რომლის მიხედვითაც კვანტურ არხში ვახდენთ გასაღების გადაცემას არის BB84, მას პრივილეგირებული ადგილი უკავია არსებულ

პროტოკოლთა სიაში: ეს ის არის, რომელსაც ყველაზე მეტად აანალიზებენ და ყველაზე ხშირად ანხორციელებენ, მათ შორის მას, რომელიც კომერციულ პროდუქტებში გამოიყენება. კიდევ ერთი გამოკვეთილი უპირატესობა რაც BB84 გამოყენებამ მოგვცა არის ის, რომ ნებისმიერი სახის მოსმენა კანონიერი მხარეებისთვის იქნება შესამჩნევი და შემდეგ ტექნიკურად ამ ფაქტის გამოსწორება შესაძლებელია. აღნიშნულიდან გამომდინარე, ჩვენ მოვხსენით გასაღებების სტრიმის გადაცემის პრობლემა.

შედეგების გამოყენების სფერო ნაშრომ გააჩნია პრაქტიკული მნიშვნელობა კიბერ უსაფრთხოების და გამოყენებადობის გამოუჯობესების კუთხით. ახალი სქემა, რომლის დიდი უპირატესობას უკვე არსებულ სხვა სქემებთან შედარებით, უსაფრთხოებისა და ეფექტურობის თვალსაზრისით. პრაქტიკულად კვანტური კომპიუტერების მოხმარებაში ჩაშვების შემთხვევაში სქემა შესაძლებელია გამოყენებული იქნას კრიფტოგრაფიული მიზნებისთვის რაც იძლევა საშუალებას დავზოგოთ კრიტიკულად მნიშვნელოვანი დრო და რესურსი.

დისერტაციის სტრუქტურა და მოცულობა. სადოქტორო ნაშრომი შედგება შესავლისგან, რვა თავისგან ორმოცდაორი ქვეთავისგან, შედეგების განსჯის, დასკვნებისგან და გამოყენებული ლიტერატურის სიისგან. ნაშრომში წარმოდგენილია 22 გრაფიკული გამოსახულება.

ნაშრომის ძირითადი შინაარსი

თავი 1. შემთხვევითი ბიტების კოდირება, ქუბიტების დახმარებით

პირველ თავში გაკეთებულია არსებული კვანტური გასაღების განაწილების კრიტიკული ანალიზი. ანალიზმა გვიჩვენა რომ კვანტური კომპიუტერები გვაძლევენ იმის საშუალებას რომ გადავცეთ გასაღები უსაფრთხოთ.

თავი 2. მოსმენის ამოცნობა.

ამ თავში მოვახდინეთ საიდუმლო გასაღების დისტილაციის ანალიზი. ამ ანალიზმა გვაჩვენა, რომ გადაცემის დროს შესაძლებელია შეფერხება და თუ შეფერხება არის დიდი მაშინ გადაგზავნა უნდა მოხდეს ხელახლა. საბოლოოდ დავადგინეთ რომ საიდუმლო გასაღები მიღებული კომფედენციალურობის გაძლიერების შემდგომ, ელისი და ბობს შეუძლიათ გამოიყენონ კრიფტოგრაფიული მიზნებისთვის. კერძოთ, მათ შეუძლიათ გასაღების გამოყენება შეტყობინების დასაშიფრათ ან საიდუმლო არხის შესაქმნელად.

თავი 3. ორ - ეტაპიანი მიდგომა

მესამე თავში გაანალიზებულია საიდუმლო გასაღების დისტილაციის ორი ეტაპი, რეკომენდაცია და კოფედენციალურობის გაძლიერება პირველი, რეკონსილიაცია უზრუნველყოფს, რომ ორივე, კლოდი და დომინიკი შეთანხმდნენ საერთო მწკრივზე Ψ, რომელიც არ არის ფარული უთუოდ. შემდეგ, კონფიდენციალურობის გაძლიერება Ψ -დან ქმნის საიდუმლო გასაღებს K -ს. არ არის საჭირო, რომ ქვემოთ განხილული ყველა თეორემა მიუდგეს დისტილაციას ორ ეტაპად. თუმცა, ეს დაყოფა საკმაოდ ბუნებრივია როგორც პრაქტიკული ისე თეორიული თვალსაზრისით.

გაკეთებულია დისტილაციის მეთოდების მახასიათებლების და აუთენთიფიცირებული საიდუმლო გსაღების ერთჯერადი დისტილაციის ანალიზი. აგრეთვე ნაჩვენებია რომ შესაძლებელია კოფიდენციალურობის გაძლიერება ჰეშ ფუნქციების საშვალებით. ნაჩვენებია

კოფედენციალუროების გაძლიერების მეთოდიკა ექსტრაქტების საშუალებით.

თავი 4. კონფიდენციალურობის გაძლიერება ჰეშ ფუნქციათა უნივერსალური ოჯახების საშუალებით.

მეოთხე თავში გაანალიზებულია ჰეშ ფუნქციების უნივერსალური ოჯახების რამდენიმე მნიშვნელოვან ასპექტს. ჩვენ გვაინტერესებს მხოლოდ ჰეშ ფუნქციების უნივერსალური ოჯახები QKD-ით წარმოებული ბიტების კონფიდენციალურობის გაძლიერების მიზნით. პირველ ნაწილში, განვმარტავთ ჩვენს მოტივაციებს, რომელიც დეტალურად გადმოსცემს ჰეშ ფუნქციათა ოჯახების მოთხოვნებს კონფიდენციალურობის გაძლიერების მოქმედების სფეროში. შემდეგ მოვიყვანეთ ოჯახთა შესახებ განმარტებები და ვაჩვენეთ თუ როგორ ერგება ისინი ჩვენს საჭიროებებს. დაბოლოს, განვიხილავთ მათ იმპლემენტაციას. გაანალიზებულია მოთხოვნები და ამორჩეულია გაძლერებისთვის შესაფერისი უნივერსალური ოჯახები.

თავი 5. ჰეშ ფუნქციების იმპლემენტაციის ასპექტები

ამ თავში გავაანალიზეთ ზემოთხსენებული ჰეშ ფუნქციების იმპლემენტაციას და შემდეგ კონცენტრაციას მოვახდენთ ორობით ველში გამრავლებაზე.

HF_3 ოჯახი მოითხოვს კვადრატული დროის შეფასებას ვინაიდან ყველა შესაძლო $k \times l$ მატრიცა მიეკუთვნება ოჯახს (თუ დავუშვებთ, რომ k პროპორციულია hl -ის). ეს ზედმეტად შენელებულია დიდი შესასვლელი და გამოსასვლელი სიდიდეებისთვის.

ფაქტიურად, ქვეჯგუფი $HF_{3,Toeplitz}$ შეიძლება აღვიქვათ როგორც კონვოლუცია და შესაბამისად შეიძლება მისი განხორციელება ფურიეს მსგავსი გარდაქმნის საშუალებით. ფაქტიურად, უმეტესობა შესაძლებელია გავრცელდეს $HF_{3,Toeplitz}$ -ზეც.

$HF_{\alpha,\beta}$-ის მოდულარული შემცირება განსაკუთრებით მარტივი გასაკეთებელია ორობით წარმომადგენლობაში, რადგან იგი მოითხოვს მხოლოდ იმას, რომ გავაუქმოთ ყველაზე მნიშვნელოვანი ბიტები. შონჰაგის

და შტრასენის ალგორითმის გამოყენების შემთხვევაში, hl სიდიდის ორი მთელი რიცხვის გამრავლება შეიძლება შესრულდეს ასიმპტომურად OK(hllogхllogхlloghl) -ში. აღწერილია ჰეშ ფუნქციების ოჯახი რომლის იმპლემენტაცია დამყარებულია ორობით ველში გამრავლებაზე, დეტალურად არის განხილული NTT-ის გამოყენებით რიცხვობრივ-თეორიული გარდაქმნა და შემდეგ გამოკვეთილია რიცხვობრივ თეორიულ გარდაქმნებზე დაფუძნებული ჰეშ ფუნქციათა ოჯახები.

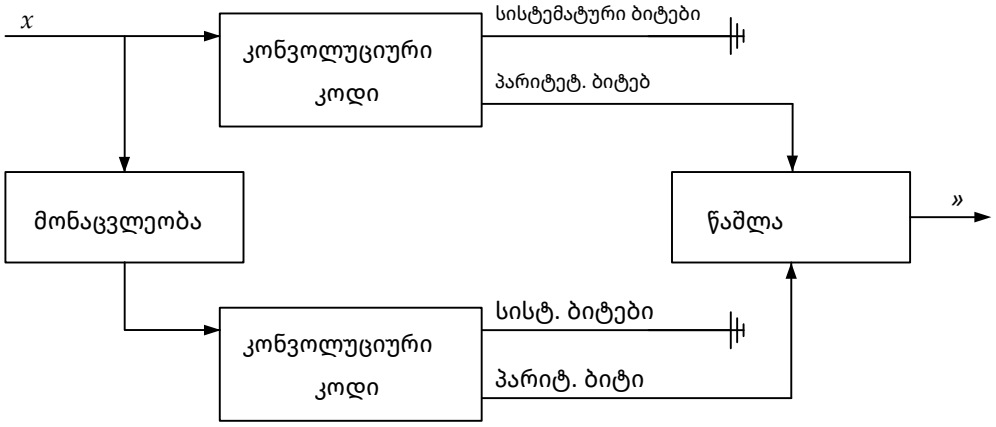
თავი 6. რეკონსილიაცია (შეთანხმება)

ამ თავში, გავაანალიზეთ შეთანხმების მეთოდების რამდენიმე კლასს. აღვწერეთ ამოცანა და რეკონსილაციის პროტოკოლის მახასიათებლები ასევე განვსაზღვრეთ შეთანხმების ძირითადი ზღვრები. აღწერილი იქნა უშეცდომობის კოდები და გრაფიკული ენტროპიები მის კავშირს მეორეხარისხოვანი მონაცემებით უშეცდომობის საწყის კოდირების ამოცანასთან მიმართებაში. ნაჩვენებია გაურკვევლობის გრაფებზე დაფუძნებულ IU და IR კოდების ექსპონენციალური - დროის ოპტიმალური დიზაინის ალგორითმი, ორობითი ინტერაქტიული შეცდომების გასწორების პროტოკოლები.

თავი 7. კონვოლუციური და ტურბო კოდები.

ამ თავში არის გაანალიზებული ტურბო და კონვოლიციური კოდები რომლებიც ტრადიციული შეცდომის გასწორების კოდებისგან განსხვავებით, მუშაობს კონკრეტული სიდიდის სიმბოლოების ბლოკებზე, კონვოლუციური კოდის შიფრატორი იღებს მის შესასვლელად ბიტების ნაკადს და უშვებს ბიტების ნაკადს. ეს დიდი უპირატესობაა შეცდომების გასწორების დროს. განხილულია ტურბო კოდების დაშიფვრა და გაშიფვრა ტურბო კოდები შედგება ორი (როგორც წესი იდენტური) კონვოლუციური კოდებისგან, რომლებიც პარალელურად ფუნქციონირებენ. მეორე კონვოლუციურ შიფრატორში შეყვანამდე, შემავალი ბიტები იცვლიან ადგილებს გადამნაცვლებელის (ინტერლივერი) საშუალებით. მონაცვლეობა ხშირად იღებს ფსევდო - შემთხვევითი გადანაცვლების ფორმას და

ავრცელებს ბიტებს ისე რომ მეორე შიფრატორი წარმოქმნის პარიტეტული ბიტების განსხვავებულ ოჯახს.



ნახაზი 1. ტურბო კოდების გაშიფვრა

ნაჩვენებია რომ ტურბო კოდების გაშიფვრა ეყრდნობა ორივე კონვოლუციური შიფრატორის რბილ დეკოდირებას. ტურბო კოდების კარგი მოქმდება მომდინარეობს იმ მეორის რბილი დეკოდირებით.

თავი 8. ახალი სქემა

ამ თავში წარმოდგენილია გაუმჯობესებული ელექტრონული ხელმოწერა. ეს მიღწეულია ჰიბრიდული მიდგომით ელექრონულ ხელმოწერად გამოიყენება ერთჯერადი ვინტერნიცის ხელმოწერა. გასაღების განაწილებისთვის ჩვენ ვიყენებთ BB84 პროტოკოლის აუცილებელ ეტაპებს. უნდა აღინიშნოს, რომ ხელმოწერის ზომა კლებულობს გამომდინარე იქიდან რომ არ გამოიყენება მერკლის ხელმოწერის სქემა. მოყვანილია ახალი სქემის ეფექტურობის ანალიზი აგრეთვე წარმოდგენილია უსაფრთხოების დამტკიცება.

ვენტერნიცის ერთჯერადი ხელმოწერის სქემა

მიუხედავად იმისა რომ გასაღების და ხელმოწერის გენერაცია LD-OTS ეფექტურია, ხელმოწერის ზომა საკმაოდ დიდია. უენტერნიცის ერთჯერადი ხელმოწერის სქემა OTS (W-OTS) რომელსაც წარმოვადგენთ ამ პარამეტრში უკეთესია მისი ზომა ხელმოწერის შემთხვევაში მნიშვნელოვნად პატარაა. იდეა მდგომარეობს იმაში, რომ გამოვიყენოთ ერთი სტრიქონი ერთჯერადი

ხელმოწერის გასაღებში, რამოდენიმე ბიტის ერთდროული ხელმოწერისთვის დაჰეშილ შეტყობინებაში. მეთოდი შემოთავაზებული იქნა მერკელის მიერ 1979 წელს.

როგორც ლაპორდი-დიფფი ერთჯერადი ხელმოწერის სქემა (LD-OTS) ასევე უენტერნიცის ერთჯერადი ხელმოწერის სქემა (W-OTS) იყენებს ცალმხრივ ფუნქციას.

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

და კრიფტოგრაფიული ჰეშ ფუნქციას.

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

W-OTS გასაღებების წყვილების გენერაცია. უნტერნიცის-ის პარამეტრი $w \geq 2$ არჩეულია ბიტების რაოდენობა, რომელიც მოწერილი იქნება ერთდროულად. შემდეგ

$$t_1 = \left\lceil \frac{n}{w} \right\rceil, \; t_1 = \left\lceil \frac{\log_2 t_1 + 1 + w}{w} \right\rceil, \quad t = t_1 + t_2 \,. \tag{6}$$

არის დეტერმინირებული. შემდეგ ხელმოწერის გასაღები X არის

$$X = (x_{t-1}, \dots, x_1, x_0) \in_R \{0,1\}^{(n,t)} \,. \tag{7}$$

სადაც ბიტების სტრინგი x_i არჩეული თანაბრად და შემთხვევითობის მეთოდით.

ვერიფიკაციის გასაღები Y გამოითვლება f ფუნქციის გამოყენებით ყოველი ბიტური სტრიქონი ხელმოწერის გასღების $2^W - 1$. ანუ ჩვენ გვაქვს.

$$Y = \left(y_{t-1}, \dots, y_1, y_0\right) \in_R \{0,1\}^{(n,t)} \tag{8}$$

სადაც

$$y_i = f^{2^w - 1}(x_i), 0 \leq i \leq t - 1. \tag{9}$$

გასაღების გენერაციისთვის საჭიროა $t = (2^w - 1)$ შეფასება f იდან და ხელმოწერის და ვერიფიკაციის გასაღების სიგრძე შესაბამისად არის $t * n$ ბიტი.

W-OTS ხელმოწერის გენერაცია. Mes შეტყობინება ჰეშით $g(Mes) = hd = (hd_{n-1}, \dots, hd_0)$ აირს ხელმოწერა. თავიდან ნოლების მინიმალური

რაოდენობა ემატება hd-ს ისე რომ მისი სიგრძე გაიყოს w-ზე. მიღებული სტრიქონი hd გაყოფილია t_1 ბიტურს სტრიქონზე $hb_{t-1}, \dots, hb_{t-t_1}$ სიგრძიდან w . შემდეგ

$$hd = hb_{t-1} \| \dots \| hb_{t-t_1}, \qquad (10)$$

სადაც || წარმოადგენს კონკატენციას. შემდეგ ბიტების სტრიქონი არის დამოკუდებელი hb_i ადგენენ მთელ რიცხვებს $\{0,1, \dots, 2^w - 1\}$ და ამოწმებენ ჯამს

$$hc = \sum_{i=t-t_1}^{t-1} (2^w - b_i)$$

გამოითვლება. სანამ $hc \leq t_1\, 2^w$, c ბინარული წარმოდგენის სიგრძე არის ნაკლები ვიდრე

$$\lfloor \log_2 t_1\, 2^w \rfloor + 1 = \lfloor \log_2 t_1 \rfloor + w + 1. \quad (12)$$

ამ ბინარულ წარმოდგენას ემატება ნოლების მინიმალური რაოდენობა, სტრიქონი გრძელდება იქამდე სანამ ის არ გაიყოფა w. ეს დაგრძელებული სტრიქონი იყოფა t_2 ბლოკებად $hb_{t_2-1}, \dots, hb_0$, სიგრძე w. შემდეგ

$$hc = hb_{t_2-1} \| \dots \| hb_0 .$$

საბოლოოდ ხელმოწერა Mes გამოითვლება

$$\sigma = \left(f^{hb_{t-1}}(x_{t-1}), \dots, f^{hb_1}(x_1), f^{hb_0}(x_0)\right). \qquad (13)$$

ყველაზე ცუდ შემთხვევაში, ხელმოწერის გენერაცია მოითხოვს $t(2^w - 1)$ შეფასებებს f-იდან. W-OTS ხელმოწერის ზომა არის $t * n$.

W-OTS ვერიფიკაცია. ხელმწერის ვერიფიკაციისთვის $\sigma = (\sigma_{t-1}, \dots, \sigma_0)$ ბიტური სტრიქონი $hb_{t-1}, \dots, hb_0$ გამოითვლება როგროც ავხსენით წინ და შემდეგ ვამოწმებთ თუ

$$\left(f^{2^w-1-hb_{t-1}}(\sigma_{n-1}), \dots, f^{2^w-1-hb_0}(\sigma_0)\right) = \left(y_{n-1,\dots,} y_0\right). \qquad (14)$$

თუ ხელმოწერა ვალიდურია, შემდეგ $\sigma_i = f^{hb_i}(x_i)$ და შესაბამისად

$$f^{2^w-1-hb_i}(\sigma_i) = f^{2^w-1}(x_i) = y_i \qquad (15)$$

ინახავს $i = t - 1, \dots, 0$. უარეს შემთხვევაში, ხელმოწერის ვერიფიკაცია მოითხოვს $t(2^w - 1)$ შეფასებებს f-იდან.

მაგალითი : დაიუშვათ $n = 3, w = 2, f: \{0,1\}^3 \rightarrow \{0,1\}^{3,} x \rightarrow x + 1$ გაყოფილი 8-ზე და $hd = (1,0,0)$. ჩვენ ვიღებთ $t_1 = 2, t_2 = 2,$ და $t = 4$ ჩვენ ავირჩიეთ ხემოწერის გასაღები

$$X = (x_{3,}x_{2,}x_{1,}x_0) = \begin{pmatrix} 1001 \\ 1011 \\ 1010 \end{pmatrix} \in \{0,1\}^{(3,4)}$$

და გამოითვლება ვერიფიკაციის გასაღები f სამჯერ გამოყენებით ბიტური სტრქონზე X:

$$Y = (y_{3,}y_{2,}y_{1,}y_0) = \begin{pmatrix} 0010 \\ 1110 \\ 0101 \end{pmatrix} \in \{0,1\}^{(3,4)}$$

დავამატოთ ერთო ნული hd და გავყოთ დაგრძელებული ბლოკებად სიგრძით 2 შემოსავლად $hd = 01\|00$. შევამოწმოთ ჯამი hc არის $hc = (4-1) + (4-0) = 7$. წინამორბედს დავამატოთ ერთი ნული hc ბინარული წარმოდგენაში და გაზრდილი სტრიქონი გავყოთ 2 შემოსავლის სიგრძის ბლოკებად $hc = 01\|11$. ხელმოწეირს გასაღები არის

$$\sigma = (\sigma_{3,}\sigma_{2,}\sigma_{1,}\sigma_0) = (f(x_3), x_2, f(x_1), f^3(x_0) = \begin{pmatrix} 0011 \\ 0001 \\ 0001 \end{pmatrix} \in \{0,1\}^{(3,4)}.$$

ხელმოწერა ვერიფიცირდება შემდეგი გამოთვლით

$$(f^2(\sigma_3), f^3(\sigma_2), f^2(\sigma_1), \sigma_0) = \begin{pmatrix} 0010 \\ 1110 \\ 0101 \end{pmatrix} \in \{0,1\}^{(3,4)}.$$

და ადრებს ვერიფიკაციის გასაღებს Y [30].

ახალი კრიპტო სისტემა

ახალი კრიპტო სისტემის იდეა მდგომარეობს იმაში, რომ მერკლის სქემის ნაცვლად გამოყენებულ იქნას ერთჯერადი ხელმოწერის სქემა. იგი ითვალისწინებს ხელმოწერის სიგრძის შემცირებას. გასაღების გადასაცემად გამოიყენება BB84 პროტოკოლი. ერთჯერადი ხელმოსაწერის სახით ვიყენებთ ვინტერნიცის სქემას [26-30].

იმისათვის, რომ დავიწყოთ გასაღების გადაცემა, ელისი ირჩევს გასაღების ორობით ელემენტებს შემთხვევითად და დამოუკიდებლად, რომელიც აღინიშნება შემთხვევითი ცვლადით X ∈ X = {0,1}. ამ პროტოკოლში არსებობს დაშიფვრის ორი წესი, რომელიც დანომრილია HI∈{1,2}-ით. ელისი

შემთხვევითად და დამოუკიდებლად ირჩევს თუ რომელ წესს გამოიყენებს თითოეული გასაღების ელემენტისთვის.

- 1-ის შემთხვევაში, ალისა ამზადებს ქუბიტს $\{|0\rangle, |1\rangle\}$ -ის ფუძიდან, როგორიცაა

  $X \rightarrow |X\rangle$.

- 2 -ის შემთხვევაში, ალისა ამზადებს ქუბიტს $\{|+\rangle, |-\rangle\}$ -ის ფუძიდან, როგორიცაა

$$X \rightarrow 2^{-1/2}(|0\rangle + (-1)^X|1\rangle)$$

თავის მხრივ, ბობი ზომავს ან $\mathbf{Z}$ ან $\mathbf{X}$-ს, რაც იძლევა შედეგს $Y_{\mathbf{Z}}$ ან $Y_{\mathbf{X}}$, შემთხვევითად არჩევს, თუ რომელ ექსპერიმენტულ მაჩვენებელს ზომავს. წინასწარ განსაზღვრული რაოდენობის ქუბიტების გაგზავნის შემდეგ, ელისი უჩვენებს ბობს თითოეულის დაშიფვრის წესს. ისინი განაგრძობენ ეგრეთწოდებულ გაცრას, ანუ ისინი აუქმებენ გასაღების ელემენტებს რომლისთვისაც ელისმა გამოიყენა 1 შემთხვევა (ან 2 შემთხვევა) და ბობმა გაზომა Z (ან X). დანარჩენი (გაცრილი) გასაღების ელემენტებისთვის, ბობის მიერ გაცრილ ზომებს ავღნიშნავთ Y -თი.

დამკვირვებლის თვალსაზრისით, შერეული მდგომარეობები, რომელსაც ალისა აგზავნის 1 და 2 შემთხვევაში, განურჩეველია, ე.ი.

$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{\mathbf{HI}}{2}$.

შედეგად, რა სტატისტიკაც არ უნდა დააგროვოს ევამ, ვერანაირ მინიშნებას ვერ მიიღებს, ის 1 შემთხვევის ქუბიტს ზომავს თუ 2 შემთხვევის.

BB84 -ის იმპლემენტაცია წარმოადგენს ტექნოლოგიურ გამოწვევას. მაგალითად, ერთეული ფოტონების წარმოება მარტივი საქმე არაა. მიუხედავად ამისა, ბოლოდროინდელი მიღწევები გვიჩვენებს, რომ BB84 შეიძლება განხორციელდეს არსებული ტექნოლოგიების გამოყენებით. მომდევნო გვერდებზე მიმოვიხილავთ BB84 იმპლემენტაციის რამდენიმე შემთხვევას. ამჯერად შევაჯამებთ სხვადასხვა ვარიანტებს.

პირველი, BB84 -ის მიერ დადგენილი ინფორმაციის მატარებლები იდეალურად წარმოადგენს ერთ ფოტონიან მდგომარეობებს. თუმცა, რთულია მათი წარმოება, და ალტერნატიული გამოსავალი არის სუსტი თანმიმდევრული მდგომარეობების გამოყენება, ანუ, თანმიმდევრული მდგომარეობები ფოტონების დაბალი საშუალო რიცხვით, რათა მიუახლოვდეს ერთ - ფოტონიან მდგომარეობებს. სუსტი თანმიმდევრული მდგომარეობები შეიძლება ზოგჯერ შეიცავდეს ერთზე მეტ ფოტონს, მაგრამ ასეთი შემთხვევის ალბათობის გაკონტროლება შესაძლებელია. აგრეთვე, ფოტონების შერეული წყვილები შეიძლება გამოყენებულ იქნას ინფორმაციის მატარებლების საწარმოებლად.

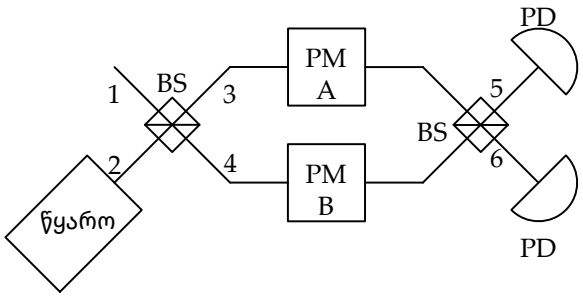
მეორე, ფოტონები შეიძლება გაიგზავნოს ან ოპტიკური ბოჭკოს საშუალებით ან საჰაერო გზით. ეს დამოკიდებულია იმაზე თუ რას ითხოვს აპლიკაცია. მაშინ როცა ოპტიკური ბოჭკო შეიძლება იყოს სატელეკომუნიკაციო ქსელების ალტერნატივა, საჰაერო საშუალება აშკარად უმჯობესი იქნება სატელიტური კომუნიკაციებისთვის.

და ბოლოს, ქუბიტის დაშიფვრა შეიძლება შესრულდეს ფოტონის პოლარიზაციაში ან მის ფაზაში. მიუხედავად იმისა, რომ ფაზური დაშიფვრა როგორც წესი სასურველია ფოტონებისთვის, რომლებიც ოპტიკურ ბოჭკოში გაედინება, პოლარიზაციული კოდირება წარმოადგენს საჰაერო საშუალების ალტერნატივას.

ფაზური დაშიფვრა

ფაზური დაშიფვრა ყველაზე პოპულარული მიდგომაა BB84 -ის განსახორციელებლად ოპტიკურ ბოჭკოში. იგი დაფუძნებულია მაჩ - ზენდერის ინტერფერომეტრზე, რომელიც ყოფს ერთეულ ფოტონს ორად, „ნახევარ“ - ფოტონებად, რომლიდანაც თითოეული გაედინება სხვადასხვა ინტერფერენციის ტრაექტორიაზე, და ორივე „ნახევარს“ აბრკოლებს.

მაჩ - ზენდერის ინტერფერომეტრი



ნახაზი 2. მაჩ - ზენდერის ინტერფერომეტრი.

წყარო (წყარო) წარმოადგენს შესასვლელს პირველი სხივ გამყოფის (BS) მე-2 მხარში, ხოლო 1 მხარი იტევს სიცარიელეს. გამომავალი განშტოებები 3 და 4 გადიან φA და φB ფაზათა გადანაცვლებას შესაბამისად ფაზურ მოდულატორებში (PMA და PMB). განშტოებები ერთდება მეორე სხივ გამყოფში (BS), რომელთა გამომავალი მხრები 5 და 6 შედის ფოტონის დეტექტორში (PD).

მოდით განვიხილოთ ნახაზი 2 -ის ექსპერიმენტი. პირველ სხივ გამყოფში შედის ერთი ფოტონი. შემავალი მდგომარეობა არის $|01\rangle_{\mathrm{nm_1 nm_2}}$ ორ - რეჟიმიან ფოკის ფუძეში, ე.ი. არც ერთი ფოტონი არ არის $\mathrm{nm_1}$ -ში და ერთადერთი ფოტონია $\mathrm{nm_2}$ -ში. დაბალანსებული სხივ გამყოფის შემთხვევისთვის, მდგომარეობა გარდაიქმნება შემდეგი სახით

$$|01\rangle_{\mathrm{nm_1 nm_2}} \rightarrow \left(|10\rangle_{\mathrm{nm_3 nm_4}} + \mathrm{i}|01\rangle_{\mathrm{nm_3 nm_4}}\right)/\sqrt{2}$$

სხივ გამყოფის შემდეგ, ალბათობის ნახევარი შედის თითოეულ ორ მხარში. არეკლილი ნაწილი გადის a $\pi/2$ ფაზათა გადანაცვლებას, ამგვარად, i მამრავლს $\mathrm{nm_4}$ -ში არსებული ფოტონისთვის. შემდეგ, ფაზათა გადანაცვლება ხდება ორ მხარში. მნიშვნელოვანია მხოლოდ ფარდობითი ფაზა $\varphi = \varphi_A - \varphi_B$, და მდგომარეობა მეორე სხივ გამყოფის შესასვლელში შეიძლება განისაზღვროს ასეთი სახით

$$\left(\mathrm{e}^{\mathrm{i}\phi/2}|10\rangle_{\mathrm{nm_3 nm_4}} + \mathrm{i}\mathrm{e}^{-\mathrm{i}\phi/2}|01\rangle_{\mathrm{nm_3 nm_4}}\right)/\sqrt{2}.$$

იგივეა არგუმეტაცია მეორე სხივ გამყოფისთვის. nm_3 -ში არსებული ფოტონი გარდაიქმნება ამგვარად $|01\rangle_{nm_3n_4} \rightarrow (i|10\rangle_{nm_5nm_6} + |01\rangle_{nm_5nm_6})/\sqrt{2}$, ხოლო ფოტონი nm_4 გარდაიქმნება ასეთი სახით $|01\rangle_{nm_3nm_4} \rightarrow (|10\rangle_{nm_5nm_6} + i|01\rangle_{nm_5nm_6})/\sqrt{2}$. ფაზათა გადანაცვლებიდან გამომდინარე $\varphi = 0, \pi/2, \pi$ or $3\pi/4$, ალგებრა უზრუნველყოფს შემდეგ გამომავალ მდგომარეობებს:

$$|\psi(\phi = 0)\rangle = i|01\rangle_{nm_5nm_6}$$
$$|\psi(\phi = \pi/2)\rangle = (i|01\rangle_{nm_5nm_6} + i|10\rangle_{nm_5nm_6})/\sqrt{2},$$
$$|\psi(\phi = \pi)\rangle = i|10\rangle_{nm_5nm_6}$$
$$|\psi(\phi = 3\pi/2)\rangle = (i|01\rangle_{nm_5nm_6} - i|10\rangle_{nm_5nm_6})/\sqrt{2}.$$

ამრიგად, მდგომარეობები მეორე სხივ გამყოფში ფორმალურად ოთხივე BB84 მდგომარეობის ექვივალენტურია,

$$|\psi(\phi = 0)\rangle = |0\rangle$$
$$\left|\psi\left(\phi = \frac{\pi}{2}\right)\right\rangle = |+\rangle$$
$$|\psi(\phi = \pi)\rangle = |1\rangle$$
$$\left|\psi\left(\phi = 3\frac{\pi}{2}\right)\right\rangle = |-\rangle$$

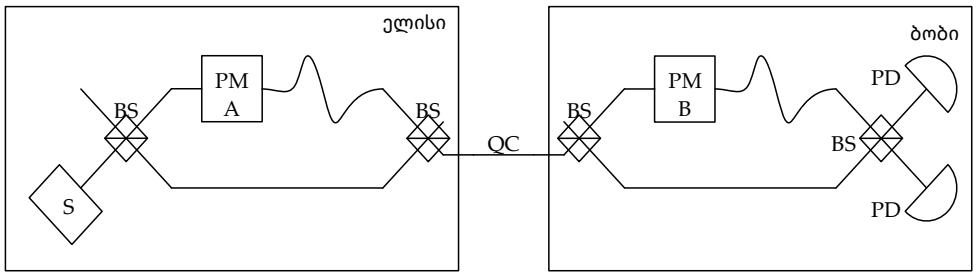
ელისი აკონტროლებს $\varphi_A \in \{0, \pi/2, \pi, 3\pi/2\}$ რათა შეარჩიოს ოთხი მდგომარეობიდან ერთ-ერთი. ბობი ყოველთვის ზომავს შემომავალ მდგომარეობას $\{|0\rangle, |1\rangle\}$ -ის ფუძეში, მიუხედავად იმისა, რომ მას შეუძლია აირჩიოს φ_B -ის სიდიდე $\{0, \pi/2\}$ -ში, რათა მოახდინოს ფუძის სელექციის იმიტაცია. დასკვნითი გაზომვა ხდება როცა

$\varphi_B = 0 \wedge \varphi_A \in \{0, \pi\}$ და $\varphi_B = \pi/2 \wedge \varphi_A \in \{\pi/2, 3\pi/2\}$.

ფაზური დაშიფვრა, როგორც ნახაზი 2-შია გამოსახული, სირთულეს წარმოადგენს, რადგან ბოჭკოვანი ოპტიკის ორი მხარის სიგრძე ზუსტად უნდა ემთხვეოდეს ტალღის სიგრძის ნაწილს. ალისას და ბობს შორის დავუშვათ ათობით კილომეტრია, ტემპერატურის ნებისმიერი ცვლილება გააფართოვებს ან შეამცირებს ბოჭკოს, სიდიდის უმნიშვნელო ხარისხით, რომელიც ტალღის სიგრძეზე გრძელია.

ამის თავიდან ასაცილებლად უნდა გამოვიყენოთ მაჩ-ზენდერის კონსტრუქცია, რომელიც ნახაზი 3-ზეა ასახული. ინტერფერომეტრები გაუწონასწორებელია, ანუ, მათ მხრებს არ აქვს თანაბარი სიგრძე. ელისის

მიერ გამოცემული ფოტონი შეიძლება რომ გაედინოს ან ორ გრძელ მხარში, ორ მოკლე მხარში ან ერთ მოკლე და ერთ გრძელ მხარში.



ნახაზი 3. ორმაგი მაჩ - ზენდერის ინტერფერომეტრი.

ალისას სადგური მოიცავს ფოტონის წყაროს (S), პირველ სხივ გამყოფს (BS), ფაზურ მოდულატორს (PMA) და მეორე სხივ გამყოფს (BS). გაითვალისწინეთ, რომ ზედა განშტოება ქვედა განშტოებაზე გრძელია. სიგნალები ერთიანდება და იგზავნება კვანტური არხის მეშვეობით (QC). ბობის სადგური ალისის სადგურის მსგავსია განსხვავებული ფაზური მოდულატორით (PMB). გრძელი და მოკლე განშტოებები კომბინირებულია მეოთხე სხივ გამყოფის (BS) მეშვეობით. გამომავალი მხრები დაკავშირებულია ფოტონის დეტექტორებთან (PD).

მიღების მომენტი განსხვავებული იქნება და შესაბამისად, ამ შემთხვევების გარჩევა შეიძლება. გაითვალისწინეთ, რომ მიღების მომენტი იგივე იქნება ფოტონისთვის, რომელიც გაედინება ჯერ გრძელ მხარში და შემდეგ მოკლე მხარში ან პირიქით. აქედან გამომდინარე, თუ ჩვენ მხოლოდ შუა მიღების მომენტს შევხედავთ, ორი „ნახევარი“ ფოტონი განიცდის ინტერფერენციას, ერთი გადის ელისის ფაზურ მოდულატორს და ერთი გადის ბობის ფაზურ მოდულატორს. ამ ხრიკის საშუალებით, ორი „ნახევარი“ ფოტონი გაედინება იგივე კვანტურ არხში, ამრიგად, ბოჭკოს დიდ ნაწილს შეიძლება ჰქონდეს სიგრძის ვარიაციები, რომელიც გავლენას არ ახდენს ინტერფერენციებზე. ყურადღებით უნდა მოხდეს მხოლოდ იმ ნაწილების სიგრძის გაკონტროლება ან კომპენსირება რომელიც შეესაბამება დაუბალანსებელ ინტერფერომეტრებს.

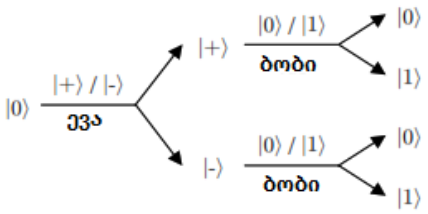
მოსმენის ამოცნობა.

აუცილებელია შევამოწმოთ მოსმენილია თუ არა ჩვენი გასაღები. შემოწმება ხორციელდება შემდეგნაირად:

მოსმენის ამოცნობის ძირითადი მახასიათებელი არის ის ფაქტი, რომ ინფორმაცია დაშიფრულია არა - ორთოგონალურ ქუბიტებში. ევას რა თქმა უნდა შეუძლია დაიჭიროს კვანტური მწკრივი და სცადოს მისი გაზომვა. მაგრამ ბობის მსგავსად, მან არ იცის წინასწარ რომელი მწკრივის წყვილი აირჩია ელისამა ყველა ძირითადი ელემენტისთვის. ბობს და ევას წარმატებით შეუძლია აირჩიოს $|0\rangle$და $|1\rangle$, როცა ელისი იყენებს $|+\rangle$ და $|-\rangle$ ან პირიქით.

კვანტურ მექანიკაში ზომები დესტრუქციულია. ნაწილაკის გაზომვის შემდეგ, შედეგს ვიღებთ პირობის სახით. უფრო ზუსტად რომ ვთქვათ, დავუშვათ, რომ დამკვირვებელი ზომავს ქუბიტს $|\phi\rangle$ რათა განასხვავოს $|0\rangle$ და $|1\rangle$. გაზომვის შემდეგ ქუბიტი გახდება $|\phi\rangle \rightarrow |\phi'\rangle = |0\rangle$ ან $|\phi\rangle \rightarrow |\phi'\rangle = |1\rangle$, გაზომვის შედეგიდან გამომდინარე, არ აქვს მნიშვნელობა თუ რომელი იყო, სანამ ქუბიტი არ იქნება ის ერთ-ერთი მათგანი რისი გამორჩევაც სურს დამკვირვებელს (მაგალითად,$|0\rangle$ ან $|1\rangle$). ყველა შემთხვევაში, როდესაც ევა იჭერს ფოტონს, ის ზომავს მას და უგზავნის ბობს, მას აქვს ¼ შეცდომის ალბათობა ალისას და ბობის ბიტებს შორის.

მოდით უარვყოთ ეს შემთხვევა. ევას აქვს ½ ალბათობა სწორი წყვილის გასაზომად. როდესაც ევა ამას აკეთებს ის არ ეხება მდგომარეობას და რჩება შეუმჩნეველი. მაგრამ ის ყოველთვის იღბლიანი არ არის. მიუხედავად ამისა, როცა ის ზომავს არასწორ სიმრავლეს, ის ბობს უგზავნის არასწორ პოზიციას (მაგ.$|+\rangle$ან$|-\rangle, |0\rangle$ან$|1\rangle$ ნაცვლად ამისა). სიტუაცია აღწერილია ნახაზში 1.4. არასწორი პოზიციისას, ბობი ძირითადად ზომავს შემთხვევით ბიტს, რომელსაც გააჩნია ალისას ბიტთან დამთხვევის ½ ალბათობა და შეცდომის ½ ალბათობა.



ნახაზი 4. სავარაუდო შედეგები, როცა ევა იყენებს მოსმენის არასწორ ზომებს

შესაბამისად, როცა ევა ცდილობს მოსმენას, ის იღებს არარელევანტურ შედეგს დაახლოებით ½ შემთხვევებში. მან შეიძლება მიიღოს გადაწყვეტილება, რომ არ მიწეროს ბობს ის მდგომარეობები რისთვისაც მან არარელევანტური შედეგი მიიღო. მაგრამ მისთვის შეუძლებელია ანალოგიური განსხვავება გააკეთოს რადგან მან არ იცის კოდირების რა მეთოდი გამოიყენება.

ევასთვის ძირითადი ელემენტების უარყოფა სისულელეა, ვინაიდან ეს ნიმუში არ გამოიყენება იმისთვის, რომ ელისი და ბობი გასაღებად გადააქციოს. თუმცა, თუ იგი შეცვლის სიტუაციას (მიუხედავად იმისა რომ ის სცდება შემთხვევის ½ ში), ალისა და ბობი აღმოაჩენენ მის არსებობას მათ ძირითად ელემენტებში შეცდომების უჩვეულოდ დიდი რაოდენობის გამო. ბობი და ევა იგივე სირთულეს აწყდებიან ალისას მიერ გაგზავნილ ინფორმაციასთან დაკავშირებით, რადგან მათ არ იციან კოდირების რომელი წესია გამოყენებული. მაგრამ სიტუაცია არ არის სიმეტრიული ბობის და ევასთვის: ყველა სახის კომუნიკაცია აუცილებელია კლასიკურ აუთენტიფიცირებულ არხში გადანაცვლებისთვის. ეს საშუალებას აძლევს ალისას გაარკვიოს, რომ ის ესაუბრება ბობს და არა ევას. შესაბამისად, კანონიერი მხარეები გარანტიას იძლევიან, რომ ევა ვერ შეძლებს გავლენა მოახდინოს გადანაცვლების პროცესზე. ამრიგად, ელისის და ბობს მხოლოდ

ძირითადი ელემენტების შედარება შეუძლიათ, რომლებიც სწორად გაიზომა. მსმენელის არსებობის დასადგენად, ელისმა და ბობმა უნდა შეძლონ გადაცემის შეცდომების გამოვლენა. ამის გასაკეთებლად, არსებობს გზა გადანაცვლებული გასაღების ნაწილის გასახსნელად. მოცემულ პროტოკოლს შეუძლია გვიჩვენოს $hl + nm$ გასაღების ელემენტი გადაცემის შემდეგ (მაგ. l+nm = 100,000) ინდექსირებული 0 -დან l + nm -1, ალისა შემთხვევითად ირჩევს nm ინდექსს (მაგ.nm = 1000) შემდეგ უკავშირდება ბობს. შემდეგ ალისა და ბობი ხსნიან სათანადო nm გასაღების ელემენტებს, რათა დათვალონ შეცდომების რაოდენობა, ნებისმიერი შეცდომა ნიშნავს იმას რომ ადგილი ჰქონდა მოსმენას. შეცდომების არარსებობა გვაძლევს გარკვეულ სტატისტიკურ დამაჯერებლობას, რომ მოსმენას საერთოდ არ ჰქონია ადგილი. მაგრამ არ არის გამორიცხული, რომ ევას გაუმართლა ან გამოიცნო კოდირების წესი ან შეცდომა დაუშვა სხვა გასაღების ელემენტებზე. რა თქმა უნდა, შემდეგ დანარჩენი ძირითადი ელემენტები გამოიყენება საიდუმლო გასაღების შესაქმნელად.

შედეგების განსჯა

საიდუმლო გასაღების მიღება ხორციელდება შემდეგნაირად: შეცდომების გამოვლენის შემთხვევაში, ალისას და ბობს შეუძლიათ შეაჩერონ პროტოკოლი, რადგან შეცდომები შეიძლება გამოწვეული იყოს მოსმენით. უკიდურეს შემთხვევაში, ეს ხელს უშლის გასაღების შექმნას, რომელიც შეიძლება ცნობილი იყოს ოპონენტისთვის. გადაწყვეტილების ეს ნაწილი შეიძლება ცოტა რთული იყოს. პრაქტიკაში, ფიზიკური რეალიზაცია არ არის იდეალური იმიტომ რომ შეცდომები შეიძლება გამოწვეული იყოს მოსმენის გარდა, ბევრი სხვა მიზეზით, როგორიცაა კვანტურ არხში ხმაური ან დანაკარგი, კვანტური მდგომარეობის არასრული გენერირება ან არასრული დედუქცია. ასევე, შესაძლოა ევამ მოისმინა იმ დაშიფრული გასაღების მცირე ნაწილი, რაც წარმოქმნის გასაღების დანარჩენ ელემენტებს საიდუმლო გასაღების შესაქმნელად. შესაბამისად, უნდა მოიძებნოს გზა კვანტური გასაღების პროტოკოლის შესაქმნელად უფრო მდგრადი ხმაურის მისაღებად.

ალისა და ბობი თვლიან შეცდომების რაოდენობას გამოვლენილ გასაღების ელემენტებში და ამ რიცხვს ყოფენ nm-ზე რათა მიიღონ სავარაუდო ნაწილის e შეფასება. ძირითადი ელემენტების მთლიანი სიმრავლის შეცდომას, e შეფასებას ეწოდება ბიტური შეცდომების ნორმა. ამის შემდეგ, მათ შეუძლიათ დაადგინონ თუ რა ოდენობის ინფორმაციას ფლობს ევა გასაღების ელემენტების შესახებ. მაგალითად, მათ შეუძლიათ სტატისტიკურად შეაფასონ, რომ ევამ იცის l -ის არა უმეტეს IN_{EN} ბიტისა გასაღების ელემენტებში. ეს წარმოადგენს პროტოკოლის შეფასების ნაწილს. ფორმულა, რომელიც გვაძლევს IN_{EN} სიდიდეს, აქ არ არის ახსნილი. ეს არის იმ შედეგის ანალიზი თუ რისი გაკეთება შეუძლია მოსმენას კვანტური მექანიკის კანონმდებლობიდან გამომდინარე. ასევე, IN_{EN} ზუსტად არ ამცნობს ალისას და ბობს თუ რა იცის ევამ გასაღების ელემენეტებთან დაკავშირებით. ევამ შეიძლება იცოდეს ელემენტების ზუსტი მნიშვნელობა IN_{EN} ან უბრალოდ რამოდენიმე წარმოებული ფუნქციის l შედეგი, რომელიც იძლევა IN_{EN} ინფორმაციას შენონის თვალსაზრისით. ამ ეტაპზე, ალისამ და ბობმა იციან, რომ ღია გასაღების ელემენტებს აქვთ e შეცდომების სიხშირე და პოტენციურ მსმენელს აქვს IN_{EN} ინფორმაცია მათ შესახებ. კლასიკური საერთო აუთენტიფიცირებული არხით, ალისას და ბობს შეუძლიათ სცადონ კიდეც სრულიად საიდუმლო გასაღების შექმნა; ამ ნაწილს ეწოდება საიდუმლო გასაღების დისტილაცია.

საიდუმლო გასაღების დისტილაცია მოიცავს ეტაპს, რომელსაც ეწოდება შეთანხმება, რომლის მიზანია გადაცემის შეცდომების შესწორება. ეტაპი, სახელწოდებით კონფიდენციალურობის გაძლიერება, შლის ევას ინფორმაციას გასაღების სიგრძის შემცირების ხარჯზე. მოკლედ ავღწერთ ამ ორ პროცესს.

BB84 -ის შემთხვევაში, შეთანხმება როგორც წესი იღებს ინტერაქტიულ სახეს. შეცდომები შესწორდება პროტოკოლით. ალისა და ბობი მონაცვლეობით ავლენენ მათი ძირითადი ელემენტების თანაბარ ქვეჯგუფებს. როდესაც პოულობენ თანაფარდობის სხვაობას, ეს ნიშნავს, რომ

შესაბამისი ქვეჯგუფები შეიცავენ შეცდომების განუსაზღვრელ რაოდენობას. უკიდურეს შემთხვევაში, სულ მცირე ერთს. დიქოტომიის საშუალებით, მათ შეუძლიათ მონიშნონ შეცდომის ადგილმდებარეობა და შეასწორონ ის. ისინი ამ პროცესს იმეორებენ საკმარისი რაოდენობით და შედეგად ალისა და ბობი ცვლიან თანაბარ ბიტებს. საიდუმლო გასაღების დისტილაციის დროს, ყველა კომუნიკაცია ხორციელდება საერთო აუთენტიფიცირებული კლასიკური არხის საშუალებით. გახსოვდეთ, რომ ევას არ შეუძლია ამ პროცესში ჩარევა, მაგრამ შეუძლია მოუსმინოს გაცვლილ შეტყობინებებს, რომელიც ამ შემთხვევაში, მოიცავს გაცვლილ თანაბარ ბიტებს. ამრიგად, ევას ცოდნის დონე მოიცავს $IN_{EN} + |Mes|$ ბიტს, $|Mes|$ მნიშვნელობის თანაბარ ბიტებს, რომლებიც აღმოჩენილ იქნა შესწორებისას. საიდუმლო გასაღების შესანარჩუნებლად, კონფიდენციალურობის გაძლიერების იდეა მდგომარეობს იმაში, რომ გამოყენებულ იქნას ის რაც ევამ არ იცის. ალისას და ბობს შეუძლიათ გამოთვალონ გასაღების ელემენტების ფუნქცია f, რათა გაავრცელონ ევას ნაწილობრივი უცოდინრობა მთელ შედეგზე. ასეთი ფუნქცია (მაგალითად, როგორიცაა ჰეშ ფუნქცია კლასიკურ კრიფტოგრაფიაში) ირჩევა ისე, რომ თითოეული გამომავალი ბიტი დამოკიდებული იყოს შემავალი ბიტების უმეტეს ან არა უმეტეს ნაწილზე. მაგალითად, ასეთი ფუნქცია შედგება თანაბარი შემთხვევითი ქვეჯგუფის გამოსათვლელი ბიტებისგან. დავუშვათ, რომ ევამ იცის ბიტი x_1 მაგრამ არ იცის ბიტი x_2 -ის მნიშვნელობა. თუ ფუნქცია $f(x_1 + x_2) mod\ 2$, ევას არ შეუძლია გახსნას გამომავალი მნიშვნელობა სანამ ორი ალბათობა $x_1 + x_2 = 0(mod)\ 2$ და $x_1 + x_2 = 1(mod)2$ არ გათანაბრდება განურჩევლად იმისა, თუ რა მნიშვნელობა აქვს x_1-ს. ფასი, რომლის გადახაც კონფიდენციალურობისთვის გვიწევს არის ის, რომ გამომავალი საიდუმლო გასაღების სიგრძე ნაკლები უნდა იყოს ნაწილობრივი საიდუმლო გასაღების სიგრძეზე. შემოკლების ზომა დაახლოებით იმ ბიტების რიცხვის თანაბარი უნდა იყოს, რომელიც ევამ იცის და ასევე გასაღების სიდიდის შედეგისა $hl - IN_{EN} - |Mes|$ ბიტებში. გასაღების მაქსიმალური ზომის მიღება

შესაძლებელია როცა ევამ არ იცის გასაღების შემადგენელი ბიტები და (მაგალითად,$hl - IN_{EN} - |Mes| = 0$) მნიშვნელოვანია, რომ შემცირებაზე ახსნა-განმარტება მოიცავდეს რაც შეიძლება მცირე ინფორმაციას, რომელიც საკმარისი იქნება ელისისა და ბობისთვის შეძლონ ყველა შეცდომის შესწორება. გაითვალისწინეთ, რომ შეცდომები უნდა შევასწოროთ ორჯერ საიდუმლო გასაღების მიერ წარმოქმენილი ბიტების რაოდენობიდან კვანტური გადაცემის დროს. პირველ რიგში, შეცდომები უნდა მივაწეროთ მოსმენას და IN_{EN} რაოდენობას. აგრეთვე, შეცდომები უნდა შესწორდეს სწრაფად, რისთვისაც ბიტების ნაწილი უნდა გაიხსნას და ჩაითვალოს როგორც $|Mes|$. და ბოლოს, კონფიდენციალურობის გაძლიერების შემდეგ მიღებული საიდუმლო გასაღები, შეიძლება გამოყენებულ იქნას ელისისა და ბობის მიერ კრიფტოგრაფიული მიზნებისთვის. კერძოდ, მათ შეუძლიათ გამოიყენონ გასაღები შეტყობინების დასაშიფვრად ან საიდუმლო არხის შესაქმნელად.

შეტყობინების ხელმოსაწერად გენერირდება ხელმოწერის და ვერიფიკაციის გასაღებები. ამისათვის, ვინტერნიცის პარამეტრი არის hw >= 2, და იგი არის ბიტების რაოდენობის ტოლი, რომლის ხელმოწერა ერთდროულად უნდა მოხდეს. გამოთვლილ უნდა იქნას v_1=nm/hw და v_2=(log$_2 v_1$ +1+hw)/hw, v= v_1+ v_2 -თან ერთად. ხელმოწერის გასაღები X შეიცავს v სიგრძის $2nm$ შემთხვევით მწკრივებს. მისი ვერიფიკაციის გასაღები Y იგივე სიდიდისაა.

X= (x_{v-1}[0], x_{v-1}[1], x_{v-2}[0], x_{v-2}[1],…, x_0[0], x_0[1]) ∈ {0,1} ^{v,2nm} .

Y= (y_{v-1}[0], y_{v-1}[1], y_{v-2}[0], y_{v-2}[1], …, y_0[0], y_0[1]) ∈ {0,1} ^{v,2nm}, სადაც y_i=$f_o^{2\text{^}hw-1}$(x_i), და 0<=i<=v-1.

ახლა გადაცემულ უნდა იქნას ვერიფიკაციის გასაღებები, იგი სრულდება BB84 პროტოკოლის გამოყენებით. ამისათვის ხორციელდება შემდეგი: შემთხვევითი ბიტების დაშიფვრა ქუბიტების დახმარებით, მოსმენის ამოცნობა, საიდუმლო გასაღების მიღება. შეტყობინების ხელმოსაწერად, განხორციელდა ჰეშირება: hashf=k_{p-1},…, k_{p-p1}. საკონტროლო ჯამი გამოითვლება შემდეგნაირად:hc=$\sum_{i=v-v1}^{v-1}(2^{hw}-hp_i)$. იმის გათვალისწინებით,

რომ hc<= $v_1 2^{hw}$, ორობითი გამოსახულების სიგრძე არის $\log_2 v_1 2^{hw}+1$. ნულების მინიმალური რაოდენობა ემატება ორობით გამოსახულებას, რათა მივიღოთ გამოსახულების სიგრძე, რომელიც იყოფა *w*-ზე. შედეგად, იგი იყოფა *w* სიგრძის v_2 ნაწილებად. შეტყობინებაზე ხელმოწერა ხდება შემდეგნაირად: $SIG=(f_o^{p_{v-1}}(x_{v-1}), \ldots, f_o^{p_0}(x_0))$.

ხელმოწერის დასადასტურებლად, უნდა დადასტურდეს მომდევნო განტოლება: $(f_o^{(2^{hw}-1-v_{v-1})})(SIG_{nm-1}), \ldots, (f_o^{(2^{hw}-1-v_0)})(SIG_0) = y_{n-1}, \ldots y_0$.

დასკვნა

მიღებული შედეგიდან გამომდინარე, ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემას უსაფრთხოა, რადგან იგი იყენებს ვინტერნიცის ერთჯერადი სქემის კლასიკურ ვერსიას და BB84 პროტოკოლს. სისტემის გასატეხად, დაგვჭირდება ან ვინტერნიცის ერთჯერადი სქემის ან BB84 პროტოკოლის გატეხვა. თავდაპირველი თეორიებიდან გამომდინარე ორივე ერთად შეუძლებელია. ხელმოწერის ზომა არის vnm, რომელიც ბევრად ნაკლებია ვიდრე მერკლის და ლეპორდ -დიფის შემთხვევაში.

გამოქვეყნებული შრომები

- Labadze G., "BB84 PROTOCOL AS A PROTOCOL FOR QUANTUM KEY DISTRIBUTION (QKD)." Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 27-38 ISSN 25874667 Scientific Cyber Security Association (SCSA)
- Labadze G., Iavich M., Iashvili G.,Pirtskhalava I., D.Magraqvelidze "*The idea of decreasing the signature size in hash-based digital signatures"*, http://ceur-ws.org; ISSN1613-0073, extended proceedings of International Workshop on Cyber Hygiene&Conflict Management in Global Information Networks, CMiGIN 2020 (accepted for publication)
- Labadze G., Iavich M., Iashvili G.,Gagnidze A., Gantyuk S., "*Post-quantum digital signature scheme with BB84 protocol."* http://ceur-ws.org; ISSN1613-0073, extended proceedings of 26th International Conference Information Society and University Studies - IVUS 2021 (accepted for publication)
- Labadze G.,G.,Pirtskhalava I., *"THE IDEAS OF REDUCING THE SIGNATURE SIZE IN HASH-BASED"* Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 29-36 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

მოხსენებები კონფერენციებზე

- International Workshop on Cyber Hygiene&Conflict Management in Global Information Networks, CMiGIN 2020*, Post-quantum digital signature scheme with BB84 protocol,* Kyiv, Ukraine.
- International Conference Information Society and University Studies - IVUS 2021, *The idea of decreasing the signature size in hash-based digital signatures,* Kaunas, Lithuania.

Abstract

Quantum and Post-Quantum cryptography

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, 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 computer-based attacks.

Digital signature has become an important technology in the security of the Internet and other IT infrastructures. Digital signature ensures authenticity, integrity and identification of data. Digital signature is widely used in the protocols of identification and authentication. Thus, the given secure digital signature algorithm has a crucial importance for supporting the IT security.

The digital signature algorithms used in practice today are RSA, DSA, ECDSA but they are not quantum resistant because their security is based on complex factorization, large composite integers and calculation of descrete logarithms.

Hash based digital signature schemes we present here, suggest very interesting alternatives. Like any other digital signature scheme, a hash based digital signature scheme uses a cryptographic hash function.

Their security depends on the collision resistance of hash function. In fact here is presented a hash –based digital signature scheme, which is secure only when the basis of the hash function is resistant to collision. The existence of collision resistant hash function can be seen as a minimum requirement for the signature scheme, which can mark (sign) many documents with a single personal key. This signature scheme means digital signature (array of bits with fixed length) of documents (long array of arbitrary bits). It shows that digital signature is actually a hash function. These hash functions must be resistant to collision: if it is possible to create two documents with the same digital signature, the signature scheme can no longer be considered secure. This argument shows that there exists a hash based digital signature scheme as long as there is any digital signature scheme, which can sign several documents with a single key. Consequently, hash – based signature is an important candidate for the post – quantum signature. However, their resistance to quantum computers has not been proved, the requirements for their security are minimal. Despite this, every new cryptographic scheme gives us a new signature scheme. Thus, the creation of secure circuits is independent of complex algorithms, number theory and algebra. They meet the constructions from symmetric cryptography. This is one more great advantage of hash – based signature scheme. The described hash function can be chosen in consideration of hardware, software resources. For example, the signature scheme should be implemented on a chip on which AES has been implemented. A hash function based on AES can be used for reducing the size of the same signature scheme and for optimizing its execution time. Hash based digital signature scheme was created by Ralph Merkle. Merkle began with a single signature scheme to which Lamport and Diffie contributed partially. Single signature is quite fundamental. Single secure signature schemes require only one – sided function. Ropell shows that one – sided function is necessary and sufficient for secure digital signature. So, single signature schemes are really a fundamental type among digital signature schemes. However, they have serious drawbacks. One pair of keys consisted of a secret signature key and a public key can be used for the verification of a single document only. This is not enough for the majority

of applications. It was Merkle's idea to use a hash tree, which reduces the validity of many single keys (hash tree leaves) and authenticity of one public key (hash tree root). Merkle's primary construction is quite efficient compared to the RSA signature scheme. However, many improvements have been found since then, and this kind of approach of hash – based signature is quite successful alternative of RSA and elliptic curve signature schemes.

Transfer of quantum key is a method, which allows the two parties, conventionally Alice and Bob, to use a common secret key for cryptographic purposes. This paper is intended to show you a general idea what the quantum key transfer is and what methods it uses.

In order to ensure the privacy of the message, Alice and Bob agree on a part of shared secret information, which we call a key. Encryption occurs by means of integrating a message and a key so that the result is not clear to an interested party for whom the key is unknown. The recipient of the message uses a copy of the key to decrypt it.

This thesis analyzes several signature schemes that can be considered resistant to a quantum computer attack. However, the circuits have an efficiency problem. The most important problem with circuits is the long signatures. The serious problem of the digital signature is the size of the signature.

The thesis proposes the methodology for reducing the size of the signature, by means of integrating quantum key distribution protocol into hash based digital signature scheme. The analysis of the final scheme is offered. The proof of the security is offered.