საქართველოს ტექნიკური უნივერსიტეტი

გიორგი ლაბაძე

კვანტური და პოსტ-კვანტური კრიფტოგრაფია

წარმოდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა „ინფორმატიკა“

შიფრი 0613

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0160, საქართველო

საქართველოს ტექნიკური უნივერსიტეტი

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი
გამოთვლითი მათემატიკის დეპარტამენტი

ჩვენ, ქვემორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით გიორგი ლაბაძის მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: „კვანტური და პოსტკვანტური კრიფტოგრაფია“ და ვაძლევთ რეკომენდაციას საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

----, ----- 2021 წელი

ხემძღვანელი: პროფესორი მაქსიმ იავიჩი

რეცენზენტი:----------

რეცენზენტი:----------

საქართველოს ტექნიკური უნივერსიტეტი

2021

ავტორი: გიორგი ლაბაძე

დასახელება: „კვანტური და პოსტ-კვანტური კრიფტოგრაფია“
სადოქტორო პროგრამა: ინფორმატიკა
ფაკულტეტი: ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

ხარისხი: დოქტორი
სხდომა ჩატარდა:

ინდივიდუალური პიროვნებების ან ინსტიტუტების მიერ ზემომოყვანილი დასახელების დისერტაციის გაცნობის მიზნით მოთხოვნის შემთხვევაში მისი არაკომერციული მიზნებით კოპირებისა და გავრცელების უფლება მინიჭებული აქვს საქართველოს ტექნიკური უნივერსიტეტს.

ავტორის ხელმოწერა

ავტორი ინარჩუნებს დანარჩენ საგამომცემლო უფლებებს და არც მთლიანი ნაშრომის და არც მისი ცალკეული კომპონენტების გადაბეჭდვა ან სხვა რაიმე მეთოდით რეპროდუქცია დაუშვებელია ავტორის წერილობითი ნებართვის გარეშე.

ავტორი ირწმუნება, რომ ნაშრომში გამოყენებული საავტორო უფლებებით დაცულ მასალებზე მიღებულია შესაბამისი ნებართვა (გარდა ის მცირე ზომის ციტატებისა, რომლებიც მოითხოვენ მხოლოდ სპეციფიურ მიმართებას ლიტერატურის ციტირებაში, როგორც ეს მიღებულია სამეცნიერო ნაშრომების შესრულებისას) და ყველა მათგანზე იღებს პასუხისმგებლობას.

რეზიუმე

მონაცემთა დაშიფვრა წარმოადგენს ტრადიციული საშუალებას სხვადასხვა სახის სენსიტიური მონაცემების კომფედენციალურობის უზრუნველსაყოფად. მონაცემთა დაშიფვრას გააჩნია სხვადასხვა სახის სენსიტიური ინფორმაციის დაცვის ტრადიციული გზა. უახლოეს მომავალში მოსალოდნელია კვანტური კომპიუტერების მასიური წარმოება. კვანტურ კომპიუტერს შეუძლია კლასიკური კრიპტო სქემების გატეხვა. შესაბამისად, კლასიკური დაშიფვრის სქემები შეიძლება უსარგებლო გახდეს კვანტური კომპიუტერული თავდასხმების მიმართ. ეს საჭიროებს კვლევითი მიდგომების შემუშავებას. უნდა შეიქმნას კრიპტო სისტემები, რომლებსაც ექნებათ იმუნიტეტი კვანტური კომპიუტერული თავდასხმების მიმართ.

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 ალგორითმის აქვს გადამწყვეტი მნიშვნელობა IT უსაფრთხოების მხარდაჭერისთვის.

ციფრული ხელმოწერის ალგორითმები რომელინიც დღეს გამოიყენებია პრაქტიკაში გახლავთ RSA, DSA, ECDSA თუმცა ისინი არ არიან კვანტურად მდგრადები, რადგან მათი უსაფრთხოება დამყარებულია რთულ ფაქტორიზაციასთან, დიდი შედგენილი მთელ რიცხვებზე და დრისკრეტული ლოგარითმების გამოთვლაზე.

ჰეშზე დამყარებული ციფრული ხელმოწერის სქემები რომელიც წარმოვადგენთ, გვთავაზობს ძალან საინტერესო ალტერნატივებს. როგოც სხვა ციფრული ხელმოწერის სქემა ასევე ჰეშზე დამყარებული ციფრული ხელოწერის სქემა იყენებს კრიფტოგრაფიულ ჰეშ ფუნქციას.

მათი უსაფრთხოება დამოკიდებულია ჰეშ ფუნქციით წინაღმდეგობრივი შეჯახებით. რელაურად 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 დოკუმენტებს (თვითნებურ ბიტების გრძელ მასივი) ციფრული ხელმოწერას (ბიტების მასივი ფიქსირებული სიგრძით). ეს გვაჩვენებს რომ ციფრული ხელმოწერა სინამდვილეში გახლავთ ჰეშ ფუნქცია. ეს ჰეშ ფუნქციები უნდა იყოს წინააღმდეგობის მიმართ მდგრადი: თუ იქნება შესაძლებელია შეიქმნას ორი დოკუმენტი ერთი და იგივე ციფრული ხელმოწერით, ხელმოწერის სქემა აღარ შეიძლება ჩაითვალოს უსფრთხოთ. ეს არგუმენტი გვანახებს, რომ არსებობს ციფრული ხელმოწერის სქემა დამყარებული ჰეშზე, რამდენადაც არსებობს

ნებისმიერი ციფრული ხელმოწერის სქემა, რომლსაც შეუძლია მოაწეროს რამოდენიმე დოკუმენტი 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 არის დამოუკიდებელი რთული ალგორითმებისგან რიცხვთა თეორიიდან და ალგებრიდან. აკმაყოფილებს კონსტრუცქიები სიმეტრიული კრიფტოგრაფიიდან. ეს არის კიდევ ერთ დიდი უპირატესობა ჰეშზე დამყარებული ხელმოწერის სქემის. აღწერილი ჰეშ ფუნცქია შეიძლება არჩეული იქნას, აპარატურულ, 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 მეკლის მიერ მერკელმა დაიწყო ერჯერადი ხელმოწერის სქემით ნაწლიობრივ ლამპორტი და დიფიი. 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 აპლიკაციებიის 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). მერკლის პირველადი კონსტრუქცია არი იყო საკმარისად ეფექტური, ძირითადად RSA ხელმოწერის სქემასთან შედარებით. თუმცა მას შემდეგ მოძიებული იქნა ბევრი გაუმჯობესებები და ხელმოწერის ეს მიდგომა დამყარებული ჰეშზე, არის მეტად წარმატებული ალტერნატივა RSA და ელიფსური მრუდის ხემოწერის სქემებისკვანტური გასაღების გადაცემა, ეს არის მეთოდი რომელიც ორ მხარეს პირობითად ელისის და ბობს, აძლევს საშველებას გამოიყენონ საერთო საიდუმლო გასაღები კრიფტოგრაფიული მიზნებისთვის, ნაშრომში მინდა შეგვექმნას საერთო წარმოდგენა თუ რა არის კვანტური გასაღების გადაცემა და რა მეთოდების იყენებს ის.

იმისთვის რომ უზრუნველყოთ შეტყობინების, კომფედენციალურობა, ელისი და ბობი თანხმდებიან საერთო საიდუმლო ინფორმაციის ნაწილზე, რომელსაც ვუწოდებთ გასაღებს. შიფრაცია ხდება შეტყობინების და გასაღების გაერთიანების შედეგად ისე რომ რეზულტატი იყოს გაუგებარი

დაინტერესებული მხარისთვის, რომლისთვისაც უცნობია გასაღები. შეტყობინების მიმღები მის გასაშიფრად იყენებს გასაღების ასლს.

წინამდებარე ნაშრომი განიხილავს ხელმოწერის რამდენიმე სქემას, რომელიც შეიძლება ჩაითვალოს რეზისტენტულად კვანტური კომპიუტერის თავდასხმის მიმართ. მიუხედავად ამისა, სქემებს გააჩნიათ ეფექტურობის პრობლემა. სქემებთან დაკავშირებით ყველაზე მნიშვნელოვანი პრობლემა არის გრძელი ხელმოწერები. ციფრული ხელმოწერის სერიოზულ პრობლემას წარმოადგენს ხელმოწერის ზომა.
აღნიშნული ნაშრომი გვთავაზობს ხელმოწერის ზომის შემცირების მეთოდოლოგიას გასაღების კვანტური განაწილების პროტოკოლის ჰეშზე დაფუძნებული ციფრული ხელმოწერის სქემაში ინტეგრირების გზით. შემოთავაზებულია საბოლოო სქემის ანალიზი და უსაფრთხოების მტკიცებულება.

Abstract

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.

შინაარსი

ნახატების და დიაგრამების ნუსხა

შესავალი

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 დიდ 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.

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.

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

აღსანიშნავია ეფექტურობის ასპექტის მნიშვნელობა. დღესდღეობით ექსპერტები 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.

ნაშრომში განხილული პროცესებისა და მოდელების განხილვის დროს გამოყენებულია მეცნიერული კვლევის მეთოდები როგორებიცაა: მათემატიკური მოდელირება და სიმულაციები, შედარება/დაკვირვება.

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.

ლიტერატურის მიმოხილვა

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 [1-3].

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 ალგორითმის აქვს გადამწყვეტი მნიშვნელობა IT უსაფრთხოების მხარდაჭერისთვის [4-6].

ციფრული ხელმოწერის ალგორითმები რომელინიც დღეს გამოიყენებია პრაქტიკაში გახლავთ RSA, DSA, ECDSA თუმცა ისინი არ არიან კვანტურად მდგრადები, რადგან მათი უსაფრთხოება დამყარებულია რთულ ფაქტორიზაციასთან, დიდი შედგენილი მთელ რიცხვებზე და დრისკრეტული ლოგარითმების გამოთვლაზე [7-10].

ჰეშზე დამყარებული ციფრული ხელმოწერის სქემები რომელიც წარმოვადგენთ, გვთავაზობს ძალან საინტერესო ალტერნატივებს. როგოც სხვა ციფრული ხელმოწერის სქემა ასევე ჰეშზე დამყარებული ციფრული ხელოწერის სქემა იყენებს კრიფტოგრაფიულ ჰეშ ფუნქციას. მათი უსაფრთხოება დამოკიდებულია ჰეშ ფუნქციით წინაღმდეგობრივი შეჯახებით. რელაურად 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 დოკუმენტებს (თვითნებურ ბიტების გრძელ მასივი) ციფრული ხელმოწერას (ბიტების მასივი ფიქსირებული სიგრძით). ეს გვაჩვენებს რომ ციფრული ხელმოწერა სინამდვილეში გახლავთ ჰეშ ფუნქცია. ეს ჰეშ ფუნქციები უნდა იყოს წინააღმდეგობის მიმართ მდგრადი: თუ იქნება შესაძლებელია შეიქმნას ორი დოკუმენტი ერთი და იგივე ციფრული ხელმოწერით, ხელმოწერის სქემა აღარ შეიძლება ჩაითვალოს უსფრთხოთ. ეს არგუმენტი გვანახებს, რომ არსებობს ციფრული ხელმოწერის სქემა დამყარებული ჰეშზე, რამდენადაც არსებობს ნებისმიერი ციფრული ხელმოწერის სქემა, რომლსაც შეუძლია მოაწეროს რამოდენიმე დოკუმენტი 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 არის დამოუკიდებელი რთული ალგორითმებისგან რიცხვთა თეორიიდან და ალგებრიდან. აკმაყოფილებს კონსტრუქციები სიმეტრიული კრიფტოგრაფიიდან [11-16].ეს არის კიდევ ერთ დიდი უპირატესობა ჰეშზე დამყარებული ხელმოწერის სქემის. აღწერილი ჰეშ ფუნცქია შეიძლება არჩეული იქნას, აპარატურულ, 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 მეკლის მიერ მერკელმა დაიწყო ერჯერადი ხელმოწერის სქემით ნაწლიობრივ ლამპორტი და დიფიი. 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 აპლიკაციებიის 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). მერკლის პირველადი კონსტრუქცია არი იყო საკმარისად ეფექტური, ძირითადად RSA ხელმოწერის სქემასთან შედარებით. თუმცა მას შემდეგ მოძიებული იქნა ბევრი გაუმჯობესებები და ახლა ხელმოწერა დამყარებული ჰეშზე, არის მეტად წარმატებული ალტერნატივა RSA და ელიფსური მრუდის ხემოწერის სქემების [17-22].

ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის სქემა.

ქვემოდ აღვწერთ ხელმოწერის სქემებს რომელთა უსაფრთხოება დაფუძნებულია კოლიზიიზგან მდგრად კრიპტოგრაფიული ჰეშ ფუნქციებზე. ეს სქემები გახლავთ მნშვნელოვნად კარგი კანდიდადები პოსტკვანტური ეპოქისთვის [23-27].

ლაპორდი - დიფფი ერთჯერადი ხელმოწერის სქემა.

ლაპორდი-დიფფი ერთჯერადი ხელმოწერის სქემა (LD-OTS) წარმოადგენს: დაუშვათ n არის დადებითი მთელი რიცხვი, უსაფრთხოების პარამეტრი

ლაპორდი-დიფფი ერთჯერადი ხელმოწერის სქემაში. ლაპორდი-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 ლაპორდი-დიფფი ერთჯერადი ხელმოწერის სქემიდან შედგება 2n ბიტიანი სტრიქონებს n სიგრძის, რომელიც აირჩევიან 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

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

ანუ LD-OTS გასაღების გენერაცია მოითხოვს 2n შეფასებას F- იდან. სტრიქონი და ვერიფიკაციის გასაღები არის 2n ბიტიანი სტრიქონები n სიგრძის.

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

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

დაუშვათ $g(Mes)=hd = (hd_{n-1},...,hd_0)$ არის მესიჯის წარმოდგენა M იდან. შემდეგ LD-OTS ხელმოწერა არის

$$\sigma = (x_{n-1}[hd_{n-1}],\ldots.,x_1[hd_1]x_0[hd_0] \in \{0,1\}^{(n,n)} \quad (4)$$

ეს ხელმოწერა წარმოადგენს n ბიტ სტრიქონების თანმიმდევრობას, რომელთაგან თითეულს სიგრძეა n. შემდეგ არჩეულია ფუნქცია რომლის

მესიჯსაც წარმოადგენს d. ბიტური სტრიქონი ამ ხელმოწრაში $x_i[0]$ თუ IN ბიტ hd ში ტოლია 0, და $x_i[1]$ წინააღმდეგ შემთხვევაში. 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 მესიჯის წარდგენას $hd= (hd_{n-1},\ldots, hd_0)$ შემდეგ ის ამოწმებს

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

ხემოწერის შემოწმება მოითხოვს n შეფასებებს f- იდან.

მაგალითი 1.

დაუშვათ n =3 , $f:\{0,1\}^3 \rightarrow \{0,1\}^3$, $x \rightarrow x+1 \bmod 8$, და დაუშვათ

hd = (1, 0, 1) M არის მესიჯის ჰეშ მნიშვნელობა. ჩვენ ავირჩიეთ ხელმოწერის გასაღები

$$X = (x_2[0], x_2[1], x_1[0], x_1[1], x_0[0], x_0[1]) = \begin{pmatrix} 100110 \\ 101101 \\ 101010 \end{pmatrix} \in \{0,1\}^{(3,6)}$$

და გამოთვალე კორესპონდენციის ვერიფიკაციის გასაღები

$$Y = (y_2[0], y_2[1], y_1[0], y_1[1], y_0[0], y_0[1]) = \begin{pmatrix} 001110 \\ 000111 \\ 010101 \end{pmatrix} \in \{0,1\}^{(3,6)}$$

და ხელმოწერა

$$\sigma = (\sigma_2, \sigma_1, \sigma_0) = (x_2[1], x_1[0], x_0[1]) \begin{pmatrix} 100110 \\ 101101 \\ 101010 \end{pmatrix} \in \{0,1\}^{(3,3)}$$

მაგალითი 2. მოვიყვანოთ მაგალითი რომელიც ახდენს იღუსტრირებას თუ რატომ უნდა გამოვიყენოთ LD-OTS ხელმოწერის გასაღები მხოლოდ ერთხელ. მაგალითად n =4. დაუშვათ რომ ხელმომწერი პირი ხელს აწერს ორ შეტყობინებას $hd_1 = (1,0,1,1)$ და $hd_2 = (1,1,1,0)$ იყენებენ ერთიდაიგივე ხემოწერის ნამდვილ გასაღებს. შესაბამისად ამ შეტყობინებების ხელმოწერა არის $\sigma_1 = (x_3[1], x_2[0], x_1[1], x_0[1])$ და $\sigma_2 = (x_3[1], x_2[1], x_1[1], x_0[0])$. შემდეგ ყველამ დაინტერესების შემთხვევაში ხელმოწერის გასაღებიდან იცის $x_3[1], x_2[0], x_2[1], x_1[1], x_0[0], x_0[1]$. მას შეუძლია გამოიყენოს ეს ინფორმაცია და დააგენერიროს ვალიდური ხელმოწერა შეტყობინებებიდან $hd_3 =$

(1,0,1,0) და $hd_4 = (1,1,1,1)$. ეს მაგალითი შეიძლება განოზგადდეს წარმოებული უსაფრთხოების პარამეტრისთვის n. ასევე არაკეთილისმსურველს შეუძლია დააგენერიროს მხოლოდ ნამდვილი ხელმოწერა. მხოლოდ გარკვეული შეტყობინებების. სანამ ჰეშ ფუნქცია გამოიყენება გამოთვლებისთვის, შეტყობინება კრიფტოგრაფიულად უსაფრთხოა, მას არ შეუძლია მოძებნოს შესაბამისი შეტყობინება [28].

უენტერნიცის 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

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

არის დეტერმინირებული. შემდეგ ხელმოწერის გასაღები X არის

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

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.

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

სადაც

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

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

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

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

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

და გამოითვლება ვერიფიკაციის გასაღები f სამჯერ გამოყენებით ბიტური სტრქონზე X:

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

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].

მერკელის ხის იდენთიფიკაციის სქემა

ერთჯერადი ხელმოწერის სქემა, შემოთავაზებული ბოლო ვერსიით, არ არის გამოყენებადი, პრაკტიკული სიტუაციების უმრავლესობისთვის, რადგანაც ყოველი წყვილი გამოიყენება მხოლოდ ერთი ხელმოწერისთვის. 1979 წელს რალფ მერკელმა შემოგვთავაზა ამ პრობლემის გადაწყვეტა. მისი იდეა მდგომარეობს შემდეგში, რომ გამოვიყენოთ სრული ბინარული ჰეშ ხე, რათა შევამციროთ ვალიდურობა შემთხვევითი მაგრამ ფიქსირებული რიცხვი ერთჯერეადი ვერიფიკაციის გასაღებისა ვალიდური ერთჯერადი ღია გასაღების. ჰეშ ხის ფუძე [31-34].

მერკელის ხელმოწერის სქემა (MSS) მუშაობს ნებისმერ კრიპტოგრაფიულ ჰეშ ფუნქციასთან და ნებისმიერ ერთჯერად ხელმოწერის სქემასთან. განმარტებისთვის დაუშვათ $g: \{0,1\}^* \to \{0,1\}^n$ არის კრიპტოგრაფიული ჰეშ ფუნქცია. ჩვენ ასევე ვთვლით, რომ შეირჩა ერთჯერადი ხელმოწერის სქემა [35,36].

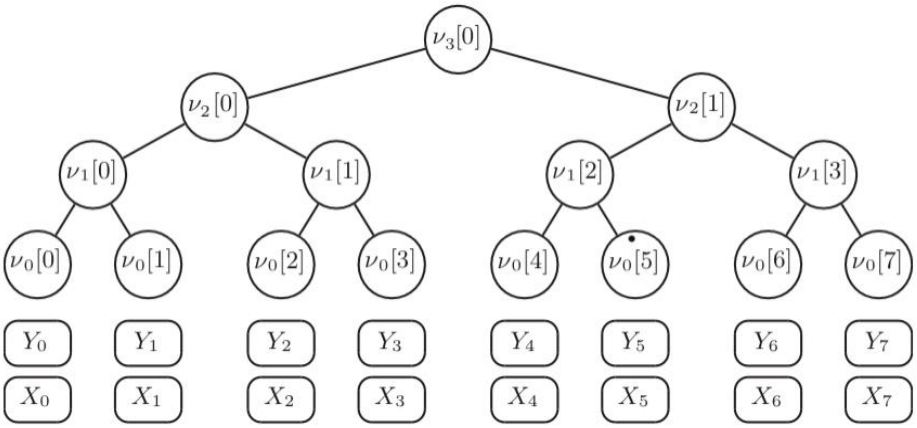
MSS გასაღებების წყვილის გენერაცია

ხელმომწერი ირჩევს $HF \in N, HF \geq 2$. შემდეგ გასაღებების წყვილი გენერირდება და მისაწვდომი იქნება ხელმოწერა/ვერიფიკაცია 2^{HF} დოკუმენტებს. აღსანიშნავია რომ არის მნიშვნელოვანი განსხვავება ისეთ ხელმოწერის სქემებთან როგორიც არის RSA და ECDSA, სადაც პოტენციურ შემთხვევით ბევრ დოკუმენტები შეიძლება ხელმოწერილ/ვერიფიცირებული იქნას ერთი წყვილი გასაღებით. თუმცა, ეს განსაზღვრული რიცხვი ასევე

შეზღუდულია მოწყობილობით რომელზეც გენერირდება ხელმოწერა ან რაიმე პოლისით. ხელმომწერი აგენერირებს 2^{HF} ერთჯერად გასაღებების წყვილს $(X_j, Y_i), 0 \leq j < 2^{HF}$. ხის შიდა კვანძები მერკელის ხეში გამოითვლება შემდეგი წესი მიხედვით: მშობელი კვანძი არის ჰეშ მნიშვნელობა, კონკატენცია მისი მარცხენა და მარჯვენა შვილების. MSS ღია გასაღების წყვილი არის მერკელის ხის ფესვი. MSS საიდუმლო გასაღები წარმოადგენს 2^{HF} ერთჯერადი გასაღებების მიმდევრობას. რომ ვიყოთ უფრო ზუსტი, მერკელის ხეში ავღნიშნოთ კვანძები [36-40]

$$\nu_h[j] = g(\nu_{h-1}[2j] || \nu_{h-1}[2j+1]), 1 \leq h \leq HF, 0 \leq j < 2^{HF-hf}. \quad (16)$$

მაგალითი მოცემულია $HF = 3$.



ნახაზი 1.

მერკელის ხე სიმაღლე $HF = 3$

MSS გასაღებების წყვილების გენერაცია მოითხოვს გამოთვლებს 2^{HF} ერთჯერადი გასაღებების წყვილიდან და $2^{HF+1} - 1$ შედარებებს ჰეშ ფუნქციას[37,38].

ფესვის ეფექტური გამოთვლები

იმისთვის რომ გამოვთვალოთ მერკელის ჰეშ ხის ფესვი, აუცილებელი არ არის შევინახოთ მთლიანი ჰეშ-ხე. ამის მაგივრად გამოიყენება ჰეშ ხის ალგორითმი 2.7, ამ ალგორითმის ძირითადი იდეა მდგომარეობს შემდეგში ფუძეების მიმდევრობით გამოვთვალოთ ბოლოები და შესაძლებლობის შესაბამისად გამოვთვალოთ მათი მშობლები. ფუძეების შესანახად ალგორითმი treehash იყენებს Stack აღჭურვილი ჩვეულებრივი push და pop

ოპერაციებით [39,30]. Treehash ალგორითმის შეყვანის შემდეგ რომლის სიმაღლეა HF მერკელის ხის. გამოსვლა არის მერკელის ხის ფუძე ანუ MSS ღია გასაღები. ალგორითმი 2.7 იყენებს

Leafcalc(j) ინსტრუქციას იმისთვის რომ გამოითვალოს j ბოლოები. Leafcalc(j) ალგორითმი 2.7 Treehash

Input: სიმაღლე HF ≥ 2

Output: მერკელის ხის ფუძე.

1. For $j = 0, \ldots, 2^H - 1\ do$

ა) გამითვალე j -ის ბოლოები: $NODE_1 \leftarrow Leafcalc\ (j)$

ბ)While $NODE_1$ აქვს იგივე სიმაღლე როგორც უმაღლეს წვერს do

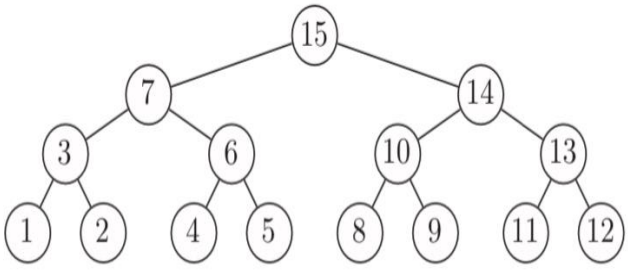
i) POP ბოლო წვერო სტეკიდან: $Node_2 \leftarrow Stak.pop()$

ii) გამოთვალე მათი მშობელი ბოლო: $Node_1 \leftarrow g(Node_2||Node_1)$

გ) Push მშობლიური ბოლო სტეკში: $Stack.push \leftarrow (||Node_1)$

2. R იყოს ერთადერთი ბოლო შენახული სტეკში: $R \leftarrow Stak.pop()$
3. დააბრუნე R.

ნახაზი 2. გვიჩვენებს მერკელის ხის კვანძების გამოთვლის წესს treehash ალგორითმის დახმარებით. ამ მაგალითში კვანძების მაქსიმალური რაოდენობა არის 3. ეს ხდება მას შემდეგ რაც დაგენერირდება 11 დაბოლოება რომელსაც $push$ - ით გაუშვებთ $Stack$ -ში. ზოგადად, treehash ალგორითმი აუცილებელია შევინახოთ უმრავლესობა HF ეგრედ წოდებული კუდი ბლოები კვანძებში. რათა გამოვთვალოთ ფუძეები მერკელის ხეში რომლის სიმაღლეა HF, treehash ალგორითმი მოითხოვს 2^{HF} -ჯერ Leafcalc გამოძახება და $2^{HF} - 1$ ჰეშ ფუნქციის გამოყენება.



ნახაზი 2. ე.წ. treehash ალგორითმი

MSS ხელმოწერის გენერაცია

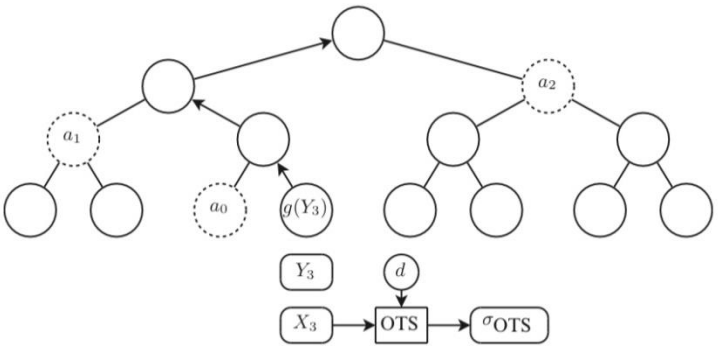
MSS თანმიმდევრულად იყენებს ერთჯერადი ხელმოწერის გასაღებს, რომ დააგენერიროს ხელმოწერა. შეტყობინება Mes ხელმოსაწერად, ხელმომწერი პირი თავიდან ითვლის n-ბიტ ჰეშს, $Hd = g(M)$, შემდეგ აგენერირებს ჰეშ ერთჯერად ხელმოწერას σ_{OTS}, sth გამოყენებით, ერთჯერადი ხელმოწერის გასაღები არის $X_s, s \in \{0, \dots, 2^{HF} - 1\}$. მერკელის ხელმოწერა მოიცავს აღნიშნულ ერთჯერად ხელმოწერას და კორესპონდენციას ერთჯერად ვერიფიკაციას Y_s. რომ დავმტკიცოთ Y_s ვერიფიკაციის აუთენტურობა, ხელმომწერი ასევე რთავს ინდექს s, ასევე აუთენტიფიკაციის გზა ვერიფიკაციის გასაღები Y_s თვის, მერკელის ხეში ბოლოების თანმიმდევრობა $A_s = (a_0, \dots., a_{H-1})$. ეს აუთენთიფიკაციის ინდექსების გზა, საშვალებას აძლევს ვერიფიკატორს აშენდეს უმოკლესი გზა ხის ბოლოდან მის ფესვამდე. ბოლო hf აუთენთფიკაციის გზაში წარმოადგენს მშობელ დაბოლოებას სიმაღლით hf გზა მერკელის ხეში ბოლოდან არის $g(Y_s)$ ფესვამდე :

$$a_{hf} = \begin{cases} v_{hf}\,[hs/2^{hf} - 1], if \lfloor hs/2^{hf} \rfloor \equiv 1\ mod\ 2 \\ v_{hf}\,[hs/2^{hf} - 1], if \lfloor hs/2^{hf} \rfloor \equiv 0\ mod\ 2 \end{cases} \qquad (17)$$

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

ნახაზი 3. ნაჩვენებია მაგალითი $s = 3$. მერკელის sth ხელმოწერა არის

$$\sigma_s = (s, \sigma_{OTS,} Y_s, (a_0, \dots., a_{Hf-1})) \qquad (18)$$



ნახაზი 3. მერკელის ხელმოწერის გენერაცია $hs = 3$. მონიშული

ბოლოები ასახავს აუთენთიფიკაციის გზას დაბოლოებამდე $g(Y_3)$. ისრები გვაჩვენებენ გზას ბოლოდან $g(Y_3)$ ფესვამდე [41,42].

მერკელის ხის ხელმოწერის ვერიფიკაცია მოიცავს ორ ეტაპის. პირველ ეტაპი ვერიფიკატორი იყენებს ერთჯერად ვარიფიკაციის გასაღებს Y_s, ერთჯერადი ხელმოწერის $\sigma_{OTS,}$ ვერიფიკაციისთვის hd გამოთვლა ხდება შემოწმების ალგორითმის დახმარებით რომელიც შესაბამისა ერთჯერადი ხელმოწერის სქემის. მეორე ეტაპზე ვერიფიკატორი ამოწმებს ვერიფიკაციის ერთჯერადი გასაღების შესაბამისობას Y_{hs} მარტივი გზით $(p_0, \dots, p_{HF})$, sth $g(Y_s)$ დაბოლოებიდან მერკელის ხის ფესვამდე. ის იყენებს ინდექს s აუთენთიფიკაცისს გზისთვის $(a_0, \dots., a_{HF-1})$ და გამოიყენება შემდეგი კონსრტუქცია.

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

$$for \; hf = 1, \dots. Hf \; \text{და} \; p_0 = g(Y_s).$$

ინდექსი hs გამოიყენება გამოიყენება იმისთვის, რომ დავადგინოთ თანრიგი და აუთენთიფიკაციის გზის კვანძები და კვანძები ბოლოდან $g(Y_s)$ მერკელის ფესვამდე რომელნიც უნდა გაერთიანდნენ. Y_s არის წარმატებული თუ hp_{HF} ტოლია საჯარო გასაღების [43,44].

კვანტური გასაღების განაწილება პირველი ეტაპი

როგორც ავღნიშნეთ, კვანტური გასაღების გადაცემა, ეს არის მეთოდი რომელიც ორ მხარეს პირობითად ელისის და ბობს, აძლევს საშველებას გამოიყენონ საერთო საიდუმლო გასაღები კრიფტოგრაფიული მიზნებისთვის, ამ თავში მინდა შეგვექმნას საერთო წარმოდგენა თუ რა არის კვანტური გასაღების გადაცემა და რა მეთოდების იყენებს ის.

იმისთვის რომ უზრუნველყოთ შეტყობინების, კომფედენციალურობა, ელისი და ბობი თანხმდებიან საერთო საიდუმლო ინფორმაციის ნაწილზე, რომელსაც ვუწოდებთ გასაღებს. შიფრაცია ხდება შეტყობინების და გასაღების გაერთიანების შედეგად ისე რომ რეზულტატი იყოს გაუგებარი

დაინტერესებული მხარისთვის, რომლისთვისაც უცნობია გასაღები. შეტყობინების მიმღები მის გასაშიფრად იყენებს გასაღების ასლს [45-48].

თავიდანვე უნდა აღინიშნოს რომ კვანტური გასაღების გადაცემის მიზანი არ არის ინფორმაციის დაშიფვრა. არამედ კვანტური გასაღების მიზანია გასაღების საუდუმლოდ გადაცემის გრანტირება. თავის მხირვ კანონიერ მხარეებს შეუძლიად გამოყენინ ეს გასაღები ინფორმაციის დასაშიფრად. გადაცემული ინფორაციის კოფედენციალურობას უზრუნველყობს ორი ასპექტი: კვანტური გასაღების გადაცემა და შიფრაციის ალგორითმი. თუ ამ ორი ასპექტიდან რომელიმე დაირღვევა, ჩაოიშლება მთელი სისტემა; შესაბამისად ჩვენ უნდა ავღნიშნოთ ორივე ასპექტის ძლიერი მხარეები.

პირველ, როგრო ხდება კოფედენციალურობის უზრუნველყოფა? კვანტური მექანიკის კანონებს აქვს უცნაური თვისებები, კარგი თვისებაა, მოესმენა შესამჩნევია. თუ მოსმენას რომელსაც პირობითად ევას უწოდებენ, ცდილობს ამოიცნოს გასაღები, ის იქნება შემჩნეული. კანონიერ მხარეებს შემდეგ შეუძლიათ უარი თქვან გასაღებზე, მანამ სანამ ინება გადაცემული რაიმე სახის კომფედენციალური ინფორმაცია. მეორეს მხრივ თუ მოსმენა არ იქნა აღმოჩენილი, საუდმლო გასაღების გადაცემა გარანტირებულია[49-52].

მეორე, შიფრაციის ალგორითმის უნდა ქონდეს ძლიერი თვისებები. როგროც ზემოთ ავღნიშნეთ მონაცემთა კომფედენცალურობა აბსოლიტურად გარანტირებულია, თუ დაშიფვრის გასაღები სიგრძე ტოლია გადასაგზავნი შეტყობინების სიგრძის და არ გამოყენება განმეორებით მომდევნო შეტყობინების დასაშიფრად. სწორედ აქ არის კვანტური გასაღების გადაცემა ყველაზე მეტად სასარგბლო, რადგან მას შეუძლია გადასცეს გრძელი გასაღები იმ სიხშირით რა სიხშირითაც ეს დაჭირდებათ ელისის და ბობს.

განვიხილოთ დეტალურად როგორ მუშაობს კვანტური გასაღების გადაცემა.

კვანტური გასაღების გადაცემა მოითხოვს გადაცემის არხს, რომელშიც კვანტური მატარებელი გადაეცემა ელისისგან ბობს. თეორიულად

ნებისმიერი ნაწილაკი რომელიც ემორჩილება კვანტური მექანიკის კანონებს შეიძლება იქნას გამოყენებული. პრაქტიკაში კვანტური მატარებელი ძირითადათ არის ფოტონი, სინათლის ელემენტარული ნაწილაკი, არხი შეიძლებელია იყოს ოფტიკურ ბოჭკოვანი
(მაგალითად, სატელეკომუნიკაციო ქსელები) ან ჰაერით (მაგალითად, თანამგზავრული კომუნიკაციებისთვის).

კვანტურ მატარებლებზე ელისი შიფრავს შემთხვევით ინფორმაციის ფრაგმენტებს, რომლითაგანაც ვადგენთ გსაღებს. ინფორმაცისს ეს ფრაგმენტები შეიძლება იყოს მაგალითად: შემთხვევითი ბიტები ან გაუსის მეთოდით განაწილებული შემთხვევითი რიცხვები, მაგრამ მიმდინარე დისკუსიის გასამარტივებლად, შემოვიფარგლოთ მხოლოდ ელისის მხრიდან ნოლების და ერთების გამოყენებით კოდირებისთვის. გათვალისწინეთ რასაც ელისი უგზავნის ბობს არ არის აუცილებელი იყოს შინაარსიანი. მთავარი აზრი იმაშია რომ მსმენელს არ შეუძლია არცერთი ბიტის პროგნოზირება. ძირითადათ, მას შეუძლია გამოიყენოს ფიქსირებული შაბლონი ან შემთხვევით დააგენერიროს ბიტები, მაგრამ ამის მაგივრად მოითხოვება „ნამდივლიად შემთხევითი“ ბიტები. ნამდვილად შემთხვევითი ბიტის მნიშვნელობას ავხსნით მოგვიანებით.

ელისის და ბობს შორის გადაცემის დროს შესაძლებელია ევა უსმენდეს კვანტურ არხს და შესაბამისად საიდუმლო გასაღების პოტენციურ ბიტებს. ეს ქმედება არ წარმოადგენს სეროზულ პრობლემას კანონიერი მხარეებისთვის, გამომდინარე იქიდან გამომდინარე რომ მოსმენა შესამჩნევია გადაცემის შეცდომებით. გარდა მაგისა საიდუმლო გასაღების დისტილაციის მეთოდი საშვალებას აძლევს ელისის და ბობს შეასწორონ მსგვსი შეცდომები, და შექმნან გასაღები იმ ბიტებისგან რომელიც უცნობია ევასთვის [53-58].

ელისის და ბობს გადაცემის შემოდგომ შეუძლიათ შეადარონ გაცვლილი ინფორმაცია, რათა გაიგონ ხომ არ არის შეცდომები გამოწვეული მოსმენელის ჩარევისგან. კვანტური გასაღების გადაცემა ამ პროცესისთვის მოითხოვს საერთო კლაიკური, აუთენთიფიცირებულ არხს როგროც ნაჩვენებია ნახაზი

4. -ზე. ეს კლასიკური არხი აქვს ორ მნიშვნელოვანი თვისება, საერთოობა და აუთენთიფიკაცია. ეს აუცილებლად უნდა იყოს საერთო გამოყენების, თუ ელისის და ბობს ექნებოდათ პირადი საკომუნიკაციო არხი, აღარ იქნებოდა საჭირო ინფორმაციის შიფრაცია, შესაბამისად შემოთავაზებულია საერთო მოხმარების არხი. ასევე მნიშვნელოვანია შედეგი, ნებისმიერი შეტყობინება რომელიც შეიძლება გაცვალონ ელისიმ და ბობმა შეიძლება შეიტყოს ევამ. აუთენთიფიკაციის ფუნქცია არის აუცილებელი იმისთვის რომ ელისი და ბობი დარწმუნდნენ რომ ისინი საუბრობენ ერთმანეთში. ჩვენ შეგვიძლია ჩავთვალოთ რომ ელისიმ და ბობმა იცნობენ ერთმანეთს და ვერ იქნებიან შეცდომაში შეყვნილი, თუ ევა მოჩვენებს თავს რომელიმე მათგანად. ამ ასპექტს მოგვიანებით დაუბრუნდებით [59-64].

ნახაზი 4. კვანტური გასაღების განაწილება

კვანტური გასაღების განაწილება, მოიცავს კვანტურ არხს და საერთო, კლასიკურ, ავთენთიფიცირებულ არხს. ელისი უგზავნის ბობს კვანტურ მდგომარეობას კვანტური არხის მეშვეობით . ევა შემჩნეულია მოსმენაში.

თავი 1. შემთხვევითი ბიტების კოდირება, ქუბიტების დახმარებით

კლასიკური ინფორმაციის თეორიაში ყველა შეტყობინება, რაღაც მომენტში შესაძლებელია გარდაიქმნას ნულებად და ერთებად. ამიტომ ინფორმაციის ერთეულს ეწოდება ბიტი ანუ $\{0,1\}$ ნაკრები. კვანტური მატარებელს BB84 ვერ აღვწერთ კლასიკური ტერმინებით, ამიტომ ჩვენ უნდა მოვახერხოთ ჩვენი ენის ადაფტაცია ამ ახალ პარამეტრთან. არსებობს შესაბამისობა ზოგიერთი ფიზიკური სისტემის კვანტურ მდგომარეობასა და მის მატარებელ ინფორმაციას შორის.

კვანტური მდგომარეობა ძირითადად იწერება დირაკის აღნიშვნებით, ვერტიკალურს ხაზსა და კუთხოვან ფრჩხილს შორის, როგროც $|\psi\rangle, |1\rangle$ ან $|x\rangle$; კვანტური იმფორმაციის ნაწილაკები, გამოისახებიან იგივე აღნიშვნებით.

კვანტურ თეორიასი ინფორმაციის უმცირეს ნაწილაკს წარმოადგენს ქუბიტი, ბიტის კვანტური ექვივალენტი. ფიზიკურ სისტემაში ქუბიტის შესაბამისობა არის ელექტრონის ბრუნვა ან ფოტონის პოლარიზაცია. მათემატიკურად ქუბიტი აღიწერება ორი კომპლექსური რიცხვის ნაკრებით.

$$\{\alpha|0\rangle + \beta|1\rangle : \ |\alpha|^2 + |\beta|^2 = 1 \ \ \alpha, \beta \in C\} \qquad (30)$$

$$|0\rangle \ და \ |1\rangle$$

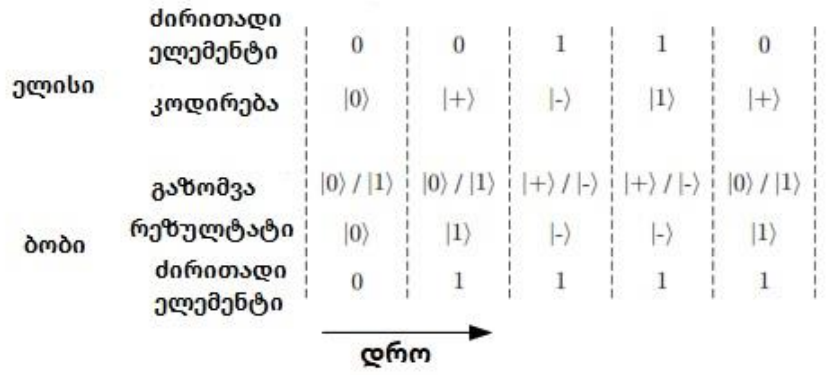
ორი საბაზო ქუბიტი, რომელიც შესაბამება ორ ორთოგონალურ მდგომარეობას კვანტურ სისტემაში. ქუბიტები $|0\rangle$ $(\alpha = 1, \beta = 0)$ და $|1\rangle$ $(\alpha = 0, \beta = 1)$ შეიძლება შევხედოთ როგორც ბიტის კვანტურ ექვივალენტს 0-ს და 1-ს შესაბამისად. α და β სხვა მნიშვნელობით ჩვენ ვამბობთ რომ ქუბიტი არის სუპერპოზიციაში $|0\rangle$ და $|1\rangle$. მაგალითად ქუბიტები $2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$ და $\sin\pi/6\,|0\rangle + \cos\pi/|1\rangle$; $|0\rangle$ და $|1\rangle$ ორივე არის სუპერპოზიციაში იმის მიუხედავად რომ განსხვავდებიან. BB84 ელისი იყენებს კოდირებას შემთხვევითი(კლასიკური) ბიტების, რომელსაც საკვანძო ელემენტები

ეწოდება ოთხი განსხვავებული ქუბიტის გამოყენებით. ბიტი 0 შეიძლება იყოს კოდირებული $|0\rangle$ ან $|+\rangle = 2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$. ბიტი 0 შეიძლება კოდირებული იყოს $|1\rangle$ ან $|-\rangle = 2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$. გავითვალისწინოთ ნიშნების განსხვავება. ორივე შემთხვევაში ელისი ირჩევს კოდირების ნებისმერ წესს შემთხვევითობის პრინციპით ალბათობის მიხედვით. შემდეგ ის აგზავნის ფოტონს არჩეული ქუბიტით ბობთან. როდესაც ფოტონი მიდის ბობის გაჩერებაზე, მას სურს გაშიფროს ის რაც ელისიმ გაუგზავნა. ამისთვის მან უნდა ჩაატაროს გაზომვები. თუმცა კვანტური მექანიკის კანონები არ აძლევს საშუალებას ბობს ბოლომდე გაშიფროს ქუბიტი. ხშირად შეუძლებელია ზუსტად გავიგოთ მიღებული ქუბიტის $\alpha|0\rangle + \beta|1\rangle$ α და β კოეფიციენტი. ამის მაგივრად ბობმა უნდა აირჩიოს ორთოგონალური ქუბიტების წყვილი და გააკეთოს გაზომვები, რომელიც ანსხვავებს მხოლოდ მათ. ჩვენ ვაბობთ რომ ორი ქუბიტი $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ და $|\psi\rangle = \alpha'|0\rangle + \beta'|1\rangle$ არის ორთოგონალური თუ $\alpha\alpha' * + \beta\beta' * = 0$.

მაგალითად ავიღოთ ორთოგონალური ქუბიტები $|0\rangle$ და $|1\rangle$. ბობს შეუძლია ჩაატაროს გაზომვები რომელიც გაარკვევს ელისის გამოგზავნილი $|0\rangle$ ან $|1\rangle$. მაგრამ რა ხდება თუ ის აგზავნის $|+\rangle$ ან $|-\rangle$? ფაქტობრივად , ბობი იღებს რეზულტატს შემთხვევით! ზოგადად თუ ბობი მიიღებს $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ ის გაზომავს $|0\rangle$ ალბათობით $|\alpha|^2$ და $|1\rangle$ ალბათობით $|\beta|^2$, დავიმახსოვროთ $|\alpha|^2 + |\beta|^2 = 1$. პრაქტიკაში $|+\rangle$ და $|-\rangle$ ბობი იღებს $|0\rangle$ და $|1\rangle$ თითეულს ალბათობით ½. მაშასადამე, ბობს არ შეუძლია განასხვავოს $|+\rangle$ და $|-\rangle$ ამ შემთხვევაში ის იღებს არაკორელირებულ ბიტების მნიშვნელობას. რა არის განსაკუთრებული ქუბიტებში $|0\rangle$ და $|1\rangle$ შეძლება ექვივალენტურად ჩაიწეროს $|0\rangle = 2^{-1/2}|+\rangle + 2^{-1/2}|-\rangle$ და

$|0\rangle = 2^{-1/2}|+\rangle - 2^{-1/2}|-\rangle$ შესაბამისად ამ შემთხვევაში, ბობს შეუძლია ელისის შეტყობინების დეკოდირება როცა ის აგზავნის $|+\rangle$ და $|-\rangle$, მაგრამ ის ვერ შეძლებს გაარჩიოს $|0\rangle$ და $|1\rangle$. ტრანსმიის დედექციის მაგალითი მოცემულია ნახაზი 1.-ზე.

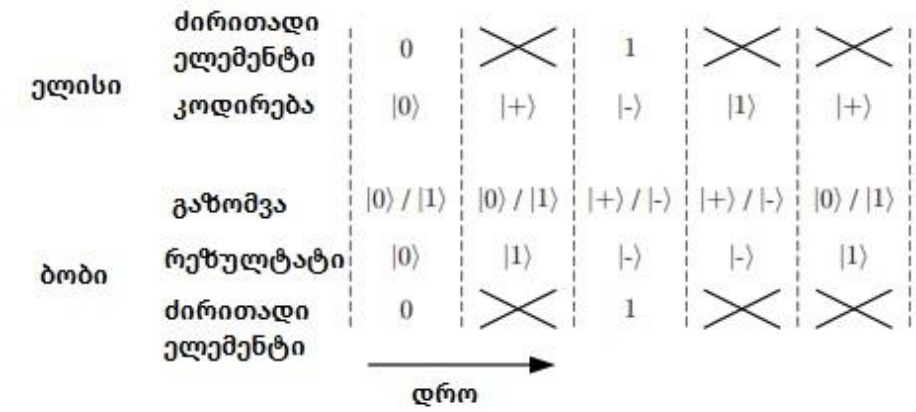
BB84 პროტოკოლში, ბობი შემთხვევით ირჩევს გაზომვებს, დაახლობით ნახევარ შემთხვევაში ის არჩევს |0⟩ და |1⟩, სხვა შემთხვევაში ის განასხვავებს |+⟩ და |−⟩. ამ ეტაპზე ელისი არ ამჟღავნებს კოდირების რომელი წესი გამოიყენა. შესაბამისად ბობი სწორად ზომავს მხოლოდ ბიტების ნახევარს, რომელიც ელისიმ გაუგზავნა მას და არ იცის რომელი მათგანია სწორი. ძირითადი ელემენტების გრძელი ნაკადის გაგზავნის შემოდგომ, ელისი ატყობინებს ბობს კოდირების წესს.



ნახაზი 5. ტრანსმისიის მაგალითი BB84 გამოყენებით.

პირველი ორი სტრიქონი არის რას აგზავნის ელისი. მესამე სტრიქონი გვაჩვენებს ბობის მიერ არჩეულ გაზომვის მეთოდს და გაზომვის შედეგად მიღებულ შესაძლო რეულტატს.

ელისიმ აირჩია ყველა ძირითადი ელემენტისთვის, ახლა ბობს შეუძლია გადაყაროს ყველა არასწორი გაზომვა; პროტოკოლის ამ ნაწილს ეწოდება გაცრა (ე.წ. შიფტინგი) რომელიც ნაჩვენებია ნახაზი 5. ზე



ნახაზი 6. ტრანსმისიის შიფტინგი

ჯერჯერობითრომ შევაჯამოთ, ელისი უგზავნის ბობს შემთხვევით ბიტებს. ელისი ირჩევს ოთხი განსხვაბევული ქუბიტისგან ბიტების კოდირებისთვის (ორი სავარაუდო ქუბიტი ბიტზე). ბობი ირჩევს ორი გაზომვის მეთოდიდან ერთერთს დეკოდირებისთვის. ბობს ყოველთვის არ შეუძლია დეტერმინირება რა გაუგზავნა ელისიმ, მაგრამ გაცრის(შიფტინგის) შემდგომ ელისი და ბობი ინახავენ ბიტების უმრავლესობას რომელთათვისაც ტრანსიმისია წარმატებით განხორციელდა. ტრანსმისის ეს სქემა ელისის და ბობს აძლევს საშუალებას შეამჩნიონ მოსმენა.

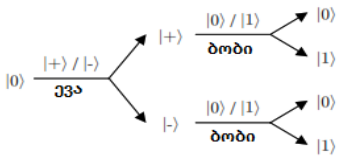
თავი 2. მოსმენის ამოცნობა

მოსმენის ამოცნობის ძირითადი თავისებურება გახლავთ ის ფაქტი, რომ ინფორმაცია კოდირებულია არაორთოგონალურ ქუბიტებში. ევას რათქმაუნდა შეუძლია დაიჭიროს კვანტური მატარებელი და სცადოს მისი გაზომვა. მაგრამ ისევე როგორც ბობმა მან არი იცის წინასწარ, მატარებლის რომელი წყვილი აირჩია ელისიმა, ყველა ძირითადი ელემენტისთვის. როგორც ბობმა ასევე ევამ შეუძლია წარუმატებლად გაარჩიოს $|0\rangle$ და $|1\rangle$ შორის, როცა ელისი იყენებს $|+\rangle$ და $|-\rangle$, ან პირიქით.

კვანტურ მექანიკაში გაზომვები დესტრუქციულია. ნაწილაკის გაზომვის შემდეგ, რეზულტატს ვიღებთ როგორც მდგომარეობას. უფრო ზუსტად, დაუშვათ 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 $|\phi\rangle \rightarrow |\phi'\rangle = |1\rangle$, დამოკიდებულია გაზომვის რეზულტატზე, მნიშვნელობა არ აქვს რა იყო $|\phi\rangle$, გარდა იმ შემთხვევისა როცა ქუბიტი არის რომელიმე მათგანი, რომელიც დამკვირვებელს სურს რომ გაარჩიოს (მაგალითად: $|0\rangle$ ან $|1\rangle$).

ყველა შემთხვევაში, როცა ევა იჭერს ფოტონს ზომავს მას და უგზავნის ბობს, მას აქვს ალბათობა ¼ შეცდომის ალბათობა ელისის და ბობის ბიტებს შორის.

მოდით დავანგრიოთ ეს შესაძლებლობა. ევას აქვს ალბათობა ½ გაზომოს სწორი წყვილი. როდესაც ევა ამას აკეთებს ის არ ეხება მდგომარეობას და რჩება შეუმჩნეველი. მაგრმა მას ყოველთვის არ უმართლებს. თუმცა როდესაც ის ზომავს არასწორ ნაკრებს, ის უგზავნის ბობს არასწორ მდგომარეობას (მაგალითად: $|+\rangle$ ან $|-\rangle$, $|0\rangle$ ან $|1\rangle$ მაგივრად). ეს სიტუაცია აღწერილია ნახაზი 7-ზე. არასწორ მდგომარეობაში ბობი ძირითადად ზომავს შემთხვევით ბიტს, რომელსაც აქვს ალბათობა ½ დამთხვევის ელისის ბიტთთან და ალბათობა ½ შცდომის.



ნახაზი 7. არასწორ გაზომვების შესაძლო შედეგები

აქედან გამომდინარე როდესაც ევა ცდილობს მოუსმინოს, ის დაახლოებით ½ შემთხვევაში იღებს არარელევანტურ შედეგს. მან შეიძლება გადაწყვიტოს არ მიწეროს ბობს მდგომარეობები, რომელთათვისაც მან მიიღო არარელევანტური შედეგი. მაგრამ მისთვის შეუძლებელია გააკეთოს მსგავსი განსხვავება, რადგან მან არ იცის კოდირების რა მეთოდია გამოყენებული.

ძირითად ელემენტებზე უარის თქმა ევასთვის უაზრობაა, რადგან ამ ნიმუში არ გამოყენებენ ელისი და ბობი გასაღების დასამზადებლად. თუმცა თუ ის მაინც მოახდენს მდგომარეობების რეტრანსლირებას (მიუხედავად იმისა, რომ ის არასწორია ½ შემთხვევაში), ელისი და ბობი აღმოაჩენენ მის არსებობას, უჩვეულოდ დიდი რაოდენობის შეცდომების გამო მათ ძირითად ელემენტებში.

ბობს და ევას აქვთ ერთი და იგივე სირთულე, ელისის გამოგზავნილ ინფორმაციასთან მიმართებაში, რადგან მათ არ იციან კოდირების რომელი წესია გამოყენებული. მაგრამ სიტაუცია არ არის სიმეტრიული ბობისთვის და ევასთვის: ყველა კომუნიკაცია, აუცილებელია შიფტინგის შესასრულებლად, კლასკურ აუთენთიფიცირებულ არხში. ეს აძლევს საშვალებას ელისის რომ გაარკვიოს ესაუბრება ბობს და არა ევას. შესაბამისად. კანონიერი მხარეები იძლევა იმის გარანტიას რომ შიფტინგის პროცესზე ევა ვერ იქონიებს გავლენას. ამრიგად ელისს და ბობს შეუძლიად მხოლოდ ის ძირითადი ელემენტები რომელიც სწორად გაიზომა. მსმენელის არსებობის

დასადგენად, ელისის და ბობს უნდა ქონდეთ საშვალება ტრანსმისიის შეცდომების აღმოჩენის. ამისთვის არის საშვალება გავხსნათ ნაწილი გაცრილი გასაღების. მოცემული პროტოკოლს შეუძლია ტრანსმისიის შემდეგ აჩვენოს $LN + nm$ ძირითადი ელემენტი(მაგალითად., l+nm =100 000) ინდექსირებული 0 დან LN+nm-1, ელისი შემთხვევით ირჩევს n ინდექსს (მაგალითად nm= 1000) შემდეგ ახდენს კომუნიკაციას ბობთან. შემდეგ ელისი და ბობი ხსნიან შესაბამის nm ძირითად ელემენტებს, რათა დაითვალონ შეცდომების რაოდენობა, ნებისმიერ შეცდომა ნიშნავს რომ იყო გარკვეული მოსმენა. შეცდომების არ არსებობა გვაძლევას გარკვეულ სტატისტიკურ ნდობას იმაზე რომ არ ყოფილა მოსმენა. მაგრამ შესაძლებელია ევას გაუმართლა, ან გამოიცნო კოდირების წესი ან დაუშვა შეცდომები სხვა ძირითად ელემენტებზე. რათქმაუნდა მაშინ დარჩენილი ძირითადი ელემენტები იქნება გამოყენებული საიდუმლო გასაღების შესაქმნელად.

2.1 საიდუმლო გასაღების დისტილაცია.

იმ შემთხვევაში, თუ შეცდომები გამოვლინდა, ელისის და ბობს შეუძლიათ გაწყვიტონ პროტოკოლი, რადგან შეცდომები შეძლება გამოწვეული იქნეას მოსმენისან. უკუდურეს შემთხვევაში ეს ხელს უშლის გასაღების შექმნას, რომელიც შეიძლება ცნობილი გახდეს მოწინააღმდეგისთვის. გადაწყვეტილების ეს მხარე შეიძლება იყოს ცოტათი მკაცრი. პრაქტიკაში ფიზიკური რიალიზაცია არ არის იდეალური, რადგან შეცდომები შეიძლება გამოწვეული იქნას ბევრი მიზეზით, გარდა მოსმენისა, ისეთი როგროიც არის მაგალითად ხმაური ან კვანტურ არხში დაკარგვა, არასრული გენერაცია კვანტური მდგომარეობის ან არასრული დედექცია. ასევე ევა შეიძლება მოისმინა პატარა ნაწილი დაშიფტული გასაღების შექმნას გასაღების დარჩენილი ელემენტები, დაშვებული საიდუმლო გასაღების შესაქმნელად. შესაბამისად უნდა გამოინახოს გზა შეიქმნას კვანტური გასაღების პროტოკოლი უფრო მდგრადი ხმაურთან მიმართებაში.

ელისი და ბობი ითვლიან შეცდომების რაოდენობას გამოვლენილ ძირითად ელემენტებში და ყოფენ ამ რიცხვს nm-ზე, რომ მიიღონ მოსალოდნელ წილადის e შეფასების მისაღებად, ძირითადი ელემენტების მთელი ნაკრების შეცდომებს, შეფასებას e ეწოდება ბიტების შეცდომის ნორმა. ამის შემდგომ მათ შეუძლიათ დაასკვნან, რამდენი ინფორმაციას ფლობს ევა ძირითად ელემენტებზე. მაგალითად მათ შეუძლიათ სტატისიკურად შეაფასონ, რომ ევამ იცის არაუმეტეს ვთქვათ IN_{EN} ბიტისა LN ძირითად ელემენტებში. ეს არის პროტოკოლის შეფასების ნაწილი. ფორმულა რომელიც გვაძლევს IN_{EN} რაოდენობას აქ არ არის განმარტებული; ეს შედეგია იმ ანალიზისა, თუ რა შეუძლია გააკეთოს მოსმენამ, კვანტური მექანიკის კანონების გათვალისწინებით. აგრეთვე IN_{EN} ზუსტად არ ეუბნება ელისის და ბობს, თუ რა იცის ევამ ძირითადი ელემენტების შესახებ. ევამ შეიძლება იცოდეს ზუსტი მნიშვნელობა IN_{EN} ელემენტების ან მხოლოდ რეზულტატი რამოდენიმე წარმოებული ფუნქციის LN . რაც აძლევს IN_{EN} ინფორმაციას შენონის გაგებით.

ამ ეტაპზე ელისიმ და ბობმა იციან, რომ გახსნილი ძირითადი ელემენტებს აქვთ e შეცდომების ნორმა და პოტენციური მსმენელს აქვს IN_{EN} ინფორმაცია მათზე. კლასიკური საერთო აუთენთიფიცირებული არხით, ელისის და ბობს შეუძლათ კიდევს სცადონ შექმნან სრულად საიდუმლო გასაღები; ამ ნაწილს ეწოდება საიდუმლო გასაღების დისტილაცია.

საიდუმლო გასაღების დისტილაცია, მოიცავს ეტაპს რომელსაც ეწოდება შეთანხმება, რომლის მიზანია გადაცემის შეცდომების შესწორება. და ნაბიჯს რომელსაც ეწოდება კომფედენციალურობის გაძლიერება, რომელიც შლის ევას ინფორმაციას გასაღების სიგრძის შემოკლების ხარჯზე. მოკლეთ აღვწერთ ამ ორ პროცესს.

BB84 შემთხვევაში, შეთანხმება ჩვეულებრივ იღებს ინტერაქტიულ სახეს, შეცდომების შესწორებს პროტოკოლი. ელისი და ბობბი ალტერნატიულად ამჟღავნებენ მათი ძირითადი ელემენტების, ტოლ ქვესიმრავლეებს. როდესაც ისინი აღმოაჩენენ თანაფარდობის სხვაობას, ეს

ნიშნავს, შესაბამის ქვესიმრავლეები შეიცავს გაურკეველი რაოდენობის შეცდომებს. შესაბამისად უკუდურეს შემთხვევაში ერთს მაინც. დიხოტომიის გამოყენებით მათ შეუძლიათ შეცდომის ადგილმდებარეობის დაფიქსირება და მისი შესწორება. ისინი იმეორებენ ამ პროცეს საკმარისი რაოდენობით და შედეგად ელისი და ბობი ცვილან ტოლ ბიტებს.

საიდუმლო გასაღბის დისტილაციისას, ყველა კომუნიკაცია ხდება საერთო აუთენთიფიცირებული კლასიკური არხით. დავიმახსოროთ რო ევას არ შეუძლია ინტერვენცია ამ პროცესში, მაგრამ მას შეუძლია მოუსმინოს გაცვილილ შეტყობინებებს. რომელიც ამ შემთხვევაში შეიცავს გაცვლილ თანაბარ ბიტებს. მაშასადამე, ევას ცოდნა მოიცავს $IN_{EN} + |Mes|$ ბიტს, $|Mes|$ მნიშვნელობის თანაბარი ბიტებით რომელიც შესწორებისას იქნა აღმოჩენილი. იმისთვის რომ გასაღები იყოს საიდუმლო, კოფედენციალურობის გაძილერების იდეა მდგომარეობს იმაში, რომ გამოვიყენოთ ის რაც არ იცის ევამ. ელისის და ბობს შეუძლიათ დაითვალო გასაღბის ელემენტების ფუნქცია f-ი, ისე რომ გაავრცელონ ნაწილობრივი ევას უცოდინაროზა მთელ რეზულტატზე. ისეთ ფუნქცია (მაგალითათ, როგროც ჰეშ ფუნქცია კლასიკურ კრიფტოგრაფიაში) ირჩევა ისე რომ თითეული გამომავალი ბიტი დამოკიდებულა შემავალი ბიტების თუ ყველა არა უმეტეს ნაწილზე. მაგალითად ასეთი ფუნქცია შედგება თანაბარი შემთხევითი ქვესიმრავლეების ბიტების გამოთვლით. დაუშვათ, რომ ევამ იცის ბიტი x_1 მაგრამ არაფერი იცის x_2 ბიტის მნიშვნელობის შესახებ. თუ f ფუნქცია $x_1 + x_2 \, mod \, 2$, ევას არ შეუძლია გახსნას გამომალი მნიშვნლობა, მანამ სანამ ორი შესაძლებლობა

$x_1 + x_2 = 0(mod)\ 2$ და $x_1 + x_2 = 1(mod)\ 2$ არის ტოლი მიუხედავად იმისა თუ რა მნიშვნელობა ექნება x_1. ფასი რომლის გადახდაც გვიწევს კოფედენცალურობის გასამყარებლად არის ის, რომ გამომავალი საიდუმლო გასაღბის სიგრძე უნდა იყოს ნაკლები ვიდრე შემავალი ნაწილობრივ საიდუმლო გასაღების სიგრძე. შემოკლების ზომა დაახლოებით ტოლია ბიტების იმ რაოდენობის რაც იცის ევამ და გასაღების ზომის რეზულტატი

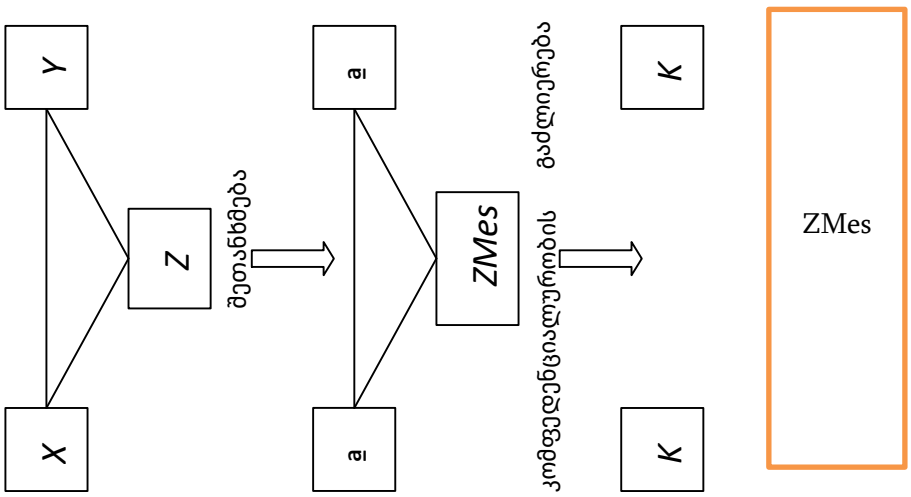
$LN - IN_{EN} - |Min|$ ბიტებში. გასაღების მაქსიმალური ზომის მისაღებად შესლებელია როცა ევამ არი იცის არაფერი გასაღების შემადგენელ ბიტებზე და შესაძლებელია რომ ყველაფერი იცის (მაგალითად $LN - IN_{EN} - |Mes| = 0$). მნიშვნელოვანია რომ გამოხშირვა, შესაძლებობის ფარგლებში ხსნიდეს მაქსიმალურად ნაკლებ ინფორმაციას, საკმარისი იმისთვის რომ ელისიმ და ბობმა შეძლონ შეასწორონ ყველა შეცდომა. მივაქციოთ ყურადღება რომ საიდუმლო გასაღბის ნაწარმოები ბიტების რაოდენობიდან უხეშად რომ ვთქვათ, კვანტური გადაცემისას შეცდომების გასწორება გვიწევს ორჯერ. პირველ რიგში შეცდომები უნდა მივაკუთნოთ მოსმენას და IN_{EN} ჩავთვალოთ. ასევე, შეცდომები უნდა იქნას სწრაფად გამოსწორებული, რისთვისაც ბიტების ნაწილი უნდა იქნას გახსინილი და ჩაითვალოს $|Mes|$.

საობოლოოდ, საიდუმლო გასაღები მიღებული კომფედენციალურობის გაძლიერების შემდგომ, ელისი და ბობს შეუძლიათ გამოიყენონ მკრიფტოგრაფიული მიზნებისთვის. კერძოთ, მათ შეუძლიათ გასაღების გამოყენება შეტყობინების დასაშიფრათ ან საიდუმლო არხის შესაქმნელად.

თავი 3. ორ - ეტაპიანი მიდგომა

როგორც ნახაზი 8. -შია ნაჩვენები, საიდუმლო გასაღების დისტილაციის პროტოკოლები ჩვეულებრივ მოიცავს ორ ეტაპს: რეკონსილიაციას (შეთანხმება) და კონფიდენციალურობის გაძლიერებას. 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.

პირველი ეტაპის სახით, რომელიც მოიცავს შეთანხმებას, კლოდმა დომინიკს უნდა გაუგზავნოს ცოტაოდენი ზედმეტი ინფორმაცია, რომელსაც ავღნიშნავთ Mes -ით. შეთანხმებული ინფორმაციის გადაცემას აკონტროლებს ევა და გათვალისწინებულ უნდა იქნას ევას ცვლადი Z' კონფიდენციალურობის გასაძლიერებლად. შემთხვევითი ცვლადი, რომელზაც ევას აქვს წვდომა აღინიშნება Z' = (Z,Mes) -ით, სადაც Z არის შეთანხმებამდე კვანტურ არხზე მიყურადებული ინფორმაცია.



ნახაზი 8. საიდუმლო გასაღების ორ -ეტაპიანი დისტილაცია

3.1 დისტილაციის მეთოდების მახასიათებლები

ამჯერად გიჩვენებთ შესაძლო გზებს საიდუმლო გასაღების დისტილაციის შესასრულებლად. ამ მეთოდებს სხვადასხვა მახასიათებლები აქვს, რომელთა განხილვაც ხდება ახლა.

პირველი, საიდუმლო გასაღების დისტილაცია შეიძლება იყოს ერთჯერადი ან განმეორებადი. პირველ რიგში, SKD პროტოკოლს აქვს მისაწვდომობა შემთხვევითი ცვლადების X და Y მხოლოდ ერთ შედეგზე (x,y) - იხილეთ აგრეთვე ნახაზი 9. მან შეიძლება გამოხატოს ერთი იმპულსის შედეგი, რომელიც გაგზავნილია კვანტური არხის საშუალებით (სადაც X და Y ჩვეულებრივ აღნიშნავს ერთ განზომილებიან ცვლადებს) ან QKD პროტოკოლის სრული სვლის საშუალებით (სადაც X და Y ჩვეულებრივ აღნიშნავს ვექტორულ ცვლადებს). განმეორებად ასპექტში SKD პროტოკოლს მისაწვდომობა აქვს ერთი და იგივე შემთხვევითი ცვლადების ბევრ დამოუკიდებელ შედეგზე $(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_n)$ ეს შესაფერისია მაშინ როდესაც QKD პროტოკოლის სვლა შეიძლება მოდელირდეს როგორც მსგავსი მოდულაციის განაწილების მქონე სვლა და როდესაც მიყურადებას თან ახლავს იგივე სტრატეგია ყოველ გაგზავნილ იმპულსზე.

ბუნებრივად, ერთჯერად SKD შედეგებს უფრო უარესი შემთხვევის მხარე აქვს ვიდრე განმეორებად SKD-ს. პირველ შემთხვევაში, კლოდმა და დომინიკმა უნდა შეძლონ კონფიდენციალურობის კონტროლი ნებისმიერ გარემოებაში, ხოლო მეორე შემთხვევაში, დიდი რიცხვების რიგი საშუალებას აძლევს მათ გაითვალისწინონ მხოლოდ საშუალო გარემოებები. მეორე, მიიჩნევა, რომ ღია კლასიკური არხი აუთენტიფიცირებულია ან არა. პირველ რიგში, პროტოკოლის მომხმარებლის პასუხისმგებლობას წარმოადგენს უზრუნველყოს ღია არხის აუთენტიფიცირება. ჩველებრივ ვვარაუდობთ, რომ კლოდი და დომინიკი უკვე მოკლე საიდუმლო გასაღებს იზიარებენ SKD პროტოკოლის გაშვებამდე, რათა მათ შეძლონ შეტყობინებების აუთენტიფიცირება SKD პროტოკოლის სრულად გასაკონტროლებლად.

მეორე შემთხვევაში, SKD პროტოკოლი უზრუნველყოფს მისი შეტყობინებების აუთენტურობას, ასე რომ აღარ უნდა გაკეთდეს დასკვნები ამ მხრივ.

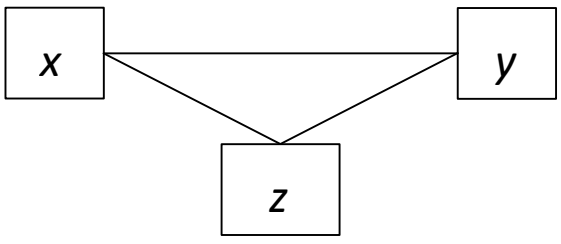
მესამე, პროტოკოლს შეუძლია ისარგებლოს ცალმხრივი ან ორმხრივი კომუნიკაციით. ცალმხრივი კომუნიკაციები მიიღება კლოდიდან დომინიკზე, რათა მოხდეს პროტოკოლის შეჯამება, რომელიც მან უნდა გაგზავნოს. ორმხრივი კომუნიკაციები ზოგადად გულისხმობს, რომ ერთი მხარე უნდა დაელოდოს მეორის შეტყობინებას სანამ რაიმეს გააგზავნის.

დაბოლოს, მოცემული შემთხვევითი ცვლადები შეიძლება იყოს დისკრეტული ან უწყვეტი.

ამ თავის დანარჩენი ნაწილი შემდეგნაირადაა ორგანიზებული. პირველად განვიხილავთ აუთენტიფიცირებული დისკრეტული SKD -ის შედეგებს (თეორემებს), დაწყებული ერთჯერადი დისტილაციიდან განმეორებად დისტილაციამდე. შემდეგ, განვმარტავთ თუ რა ხდება არა აუთენტიფიცირებული SKD -ის შემთხვევაში. დაბოლოს, ავხსნით თუ როგორ შეიძლება ზოგიერთი შედეგის გენერალიზება უწყვეტ ცვლადებზე.

3.2 აუთენტიფიცირებული საიდუმლო გასაღების ერთჯერადი დისტილაცია

ამ ნაწილში განვიხილავთ აუთენტიფიცირებული SKD -ის შემთხვევას დისკრეტული შემთხვევითი ცვლადების X, Y და Z ერთი შედეგიდან (თეორემიდან) (x,y,z), რომელიც ნაჩვენებია ნახაზზე 11. ჩვენ განვიხილავთ ორმხრივ კომუნიკაციას, თუმცა, იგი ასევე ეხება ცალმხრივ კომუნიკაციას.



ერთჯერად ასპექტში, სავარაუდოდ, კლოდს, დომინიკს და ევას აქვთ X, Y და Z შემთხვევითი ცვლადების მხოლოდ ერთი შედეგი (x,y,z).

3.3. კონფიდენციალურობის გაძლიერება ჰეშ ფუნქციების უნივერსალური ოჯახებით

ჰეშ ფუნქციების უნივერსალური ოჯახები შეიქმნა კარტერის და ვეგმანის მიერ მონაცემთა შესანახად და მოსაძიებლად. შემდგომ მოგვიანებით გაფართოვდა აუთენტიფიკაციისა და სიმრავლეთა ტოლობის მიზნებისთვის. კონფიდენციალურობის გაძლიერება ჰეშ ფუნქციათა ასეთი ოჯახებით პირველად შემოგვთავაზა ბენეტმა, ბრასარდმა და რობერტმა. საკუთარ ნაშრომში, მათ განიხილეს მიყურადების დეტერმინისტული სტრატეგიები. შემდეგ, ბენეტმა, ბრასარდმა, კრეპუმ და მაურერმა განაზოგადეს იგი მიყურადების ალბათური სტრატეგიების შემთხვევაზე.

იმისათვის რომ შევასრულოთ SKD კონფიდენციალურობის გაძლიერების საშუალებით ჰეშ ფუნქციების უნივერსალური ოჯახებით, ჩავთვალოთ, რომ კლოდი და დომინიკი ახორციელებენ რეკონსილიაციას და წინასწარ თანხმდებიან საერთო ცვლადზე Ψ. მარტივად რომ ვთქვათ, ჩავთვალოთ, რომ Ψ = X, ანუ კლოდის სიდიდე X წარმოადგენს საკონტროლო შუალედურ გასაღებს. მომდევნო შემთხვევა შეიძლება დაშვებულ იქნას უმნიშვნელოდ თუ Ψ განსაზღვრულია სხვაგვარად.

ჰეშ ფუნქციათა უნივერსალური ოჯახი, როგორც ქვემოთაა განსაზღვრული, ემსახურება მიღებული შემთხვევითი ცვლადის უნიფიცირების მიზანს.

განმარტება 2. მოცემულია სიმრავლეები HA და HB, $HA \to HB$ ფუნქციათა კლასი არის $\epsilon/|HB|$ - თითქმის 2 უნივერსალი თუ რომელიმე any $x_1 \neq x_2 \in HA$ - თვის, სიმრავლის სიდიდე $\{hf \in HF : h(x_1) = h(x_2)\}$ არის მაქსიმუმ $\epsilon|HF|/|HB|$. თუ ეს მდგომარეობა დამაკმაყოფილებელია $\epsilon=1$ -თვის, აღნიშნულ კლასს

უბრალოდ უწოდებენ 2 - უნივერსალს. მარტივად რომ ვთქვათ, ჩავთვალოთ, რომ უნივერსალი ნიშნავს 2- უნივერსალს.

მიუხედავად იმისა, რომ “almost” პარამეტრისთვის ვიყენებთ სტანდარტულ ჩანაწერს, ვსარგებლობთ ϵ ფორმულირებით, რომელიც აღნიშნავს დევიაციას უნივერსალურობიდან, გამოსასვლელი სიმრავლის სიდიდისგან $\epsilon = 1$ დამოუკიდებლად: თუ ოჯახი უნივერსალურია. ϵ, რომელიც ჩვეულებრივ გამოყენებულია ჩანაწერებში, აკმაყოფილებს $\epsilon_{\text{literature}} = \epsilon_{\text{here}}/|\text{HB}|$.

გაითვალისწინეთ, რომ 5.1.1 ნაწილში ჩვენ ვნახეთ ჰეშ ფუნქციათა ძლიერ უნივერსალური ოჯახები, რომელიც გამიზნულია აუთენტიფიკაციისთვის. კონფიდენციალურობის გაძლიერების შემთხვევაში აღარ მოითხოვება ძლიერი უნივერსალურობა, თუმცა მოითხოვება მარტივი უნივერსალურობა. ძლიერი უნივერსალურობა გულისხმობს უნივერსალურობას.

იმის გათვალისწინებით, რომ ევას არ აქვს ძალიან ბევრი ინფორმაცია (იმ გაგებით, რომელიც დაზუსტებულია ქვემოთ მოცემულ თეორემაში) X ცვლადზე, შემთხვევით შერჩეული ჰეშ ფუნქცია იძლევა შედეგს, რომელზეც ევას არა აქვს არანაირი ინფორმაცია, გარდა უმნიშვნელო ალბათობისა. მომდევნო თეორემა უმნიშვნელოდ გენერალიზდება ერთ-ერთიდან მარტივ ფაქტში, რომლისთვისაც $\epsilon \neq 1$ ასევე განხილულია შემთხვევები, რადგან მოგვიანებით დაგვჭირდება.

თეორემა 1. დავუშვათ $P_{XZ'}$ არის თავისუფალი ალბათობის განაწილება და დავუშვათ z' არის ევას მიერ შესწავლილი Z' კონკრეტული სიდიდე. თუ ევას რენის ენტროპია $HF_2(X|Z' = z')$ X-ის შესახებ ცნობილია, რომ არის სულ მცირე c და კლოდი და დომინიკი ირჩევენ $K = hf_U(X)$ საიდუმლო გასაღებად, სადაც hf_U არჩეულია შემთხვევით (ერთგვარად) ჰეშ ფუნქციათა $\epsilon/2^k$ - თითქმის უნივერსალი კლასიდან X -დან $\{0,1\}^k$ *-მდე*, სადაც X არის X *-ის* დამხმარე (support) სიმრავლე, მაშინ

$$HF(K \mid U, Z' = z') \geq (k - \log\ \epsilon) - 2^{(k-\log\ \epsilon)-c}/\ln\ 2 \qquad (31)$$

ამგვარად, ახლა გვაქვს საშუალება წავშალოთ მოწინააღმდეგის, ევას ინფორმაცია საბოლოო გასაღებზე: კლოდი და დომინიკი საჯაროდ თანხმდებიან ჰეშ ფუნქციაზე ადრე შერჩეული ოჯახიდან და შემდეგ ავრცელებენ მას X, K = $hf_U(X)$ -ზე. ჰეშ ფუნქციების უნივერსალური კლასით (ე.ი.,ϵ= 1), გამოსასვლელი ბიტების რაოდენობა უნდა შერჩეულ იქნას, ისე რომ იყოს $c \leq \min_{z'} HF_2(X|Z' = z')$- ზე ნაკლები, სხვაობა ასრულებდეს უსაფრთხოების ზღვრის ფუნქციას. გაითვალისწინეთ, რომ ორმაგი შესასვლელი შუალედებისთვის არსებობს ყველა შესასვლელი სიდიდის ჰეშ ფუნქციათა ოჯახები.

როგორც ზემოთ ავღნიშნეთ, კლოდი და დომინიკი უნდა შეთანხმდნენ იგივე შემთხვევით ცვლადზე X რეკონსილიაციით სანამ მას დაამუშავებენ ჰეშ ფუნქციის მეშვეობით. მოდით განვმარტოთ, როგორ უნდა იქნას გამოთვლილი რეკონსილიაციის მნიშვნელობა. ეს რომ დავუკავშიროთ 1 თეორემას, ლეგიტიმურმა მხარეებმა უნდა გამოთვალონ $HF_2(X|Z' = zmes)$, Z (ან *Mes*) -ის შედეგით z (ან *mes*). კაჩინმა გვიჩვენა HF2(X|Z′=zmes) ≥ HF2(X|Z=z) – |Mes| – 2hs – 2 (32)1 – 2-hs ალბათობით. აქ, |Mes| არის უბრალოდ ბიტების რაოდენობა, რომელიც გამოვლინდა რეკონსილიაციის დროს, რისი დათვლაც კლოდს და დომინიკს ადვილად შეუძლიათ. ამგვარად, მათ უნდა გამოთვალონ მხოლოდ minzHF2(X|Z = z) და დამატებით შეამცირონ გამოსასვლელი ბიტების რაოდენობა გამოვლენილი ბიტების (plus 2hs + 2) რაოდენობით. ეს მნიშვნელოვანია იმ თვალსაზრისით, რომ რეკონსილიაციის მნიშვნელობა შეიძლება გამოითვალოს კვანტურ არხზე მიყურადებისგან დამოუკიდებლად. ეს აგრეთვე ამართლებს საიდუმლო გასაღების დისტილაციის ორ - ეტაპიან მიდგომას, კერძოდ, რეკონსილიაციას, რომელსაც თან ახლავს კონფიდენციალურობის გაძლიერება. რენის ენტროპიის გამოთვლა, რომელიც საჭიროა ჰეშ ფუნქციების გამოსასვლელის სწორად გასაზომად, არ არის მარტივი ამოცანა.

მოდით შევადაროთ იგი შენონის ენტროპიას და მიმოვიხილოთ ამ შედეგების ოჯახთან მუშაობის ერთ ერთი სირთულე.

შენონის ენტროპიის ნაცვლად საზღვრების მოთხოვნის მიზეზი რენის ენტროპიაზე მდგომარეობს იმაში, რომ რენის ენტროპია რატომღაც ჯარიმას აწესებს არაერთგვაროვან განაწილებებზე. ახლა მოვიყვანთ მაგალითს იმის საჩვენებლად თუ რატომ გამოიყენება რენის ენტროპია შენონის ენტროპიის ნაცვლად. ამის საპირისპიროდ, მოდით წარმოვიდგინოთ, რომ მოყურადის ცოდნის შენონის ენტროპიაზე დაწესებულია შეზღუდვა. იმის დაშვება, რომ $HF(X|Z = z) \geq \log|X| - \epsilon$ (დავუშვათ მუდმივი X) შეიძლება ნიშნავდეს იმას, რომ ევა ϵ ბიტებს იღებს Z -გან ყოველ ჯერზე (შემთხვევა 1), ან რომ იგი იღებს სწორ სიდიდეს X *ალბათობით* $(\epsilon - 1)/(\log|X| - 1)$ და შემთხვევით სიდიდეს $X\backslash\{X\}$ -ში სხვაგვარად, თუმცა იგი არ არის ინფორმირებული თუ რომელ მოვლენას აქვს ადგილი (შემთხვევა 2). 1 შემთხვევაში, ლეგიტიმურია ჰეშ ფუნქციის გამოყენება რათა გაზარდოს ევას გაურკვევლობა, ხოლო მე -2 შემთხვევაში, ჰეშ ფუნქციის გამოყენება არ შეამცირებს მის ცოდნას იმ შემთხვევაში თუ იგი მიიღებს სწორ სიდიდეს (ე.ი. ის აწვდის სწორ ბიტებს ჰეშის ფუნქციას). რენის ენტროპიის ზედა შეფასება, მეორეს მხრივ, ხდება შენონის ენტროპიით $HF_2(X) \leq HF(X)$, რომელთა ტოლობა ხდება მხოლოდ ერთგვაროვანი განაწილების შემთხვევაში. 2 შემთხვევაში, მარტივია დავადასტუროდ, რომ $HF_2(X|Z = z) \ll H(FX|Z = z)$, ასე რომ რენის ენტროპია სწორად განიხილავს ამ შემთხვევას. რენის ენტროპიის პარადოქსული თვისება შენონის ენტროპიისგან განსხვავებით არის ის, რომ შეიძლება მოხდეს $HF2(X|Y)>HF2(X)$. კონფიდენციალურობის გაძლიერების შემთხვევაში, ეს შეიძლება ნიშნავდეს იმას, რომ რენის ენტროპიის გამოთვლა პესიმისტური მიდგომაა იმის მიმართ რაც ნამდვილად შესაძლებელია, განვიხილოთ შემდეგი დასაფიქრებელი ექსპერიმენტი: მოსმენილი ინფორმაციის Z გარდა, მისი წარმოსახვა ევას აძლევს მეორე ცვლადს Zextra რომელიც დაკავშირებულია X და Z -თან, ისე რომ $HF2(X|ZZextra) > HF2(X|Z)$.

ევა შეუძლია არ გამოიყენოს ეს დამატებითი ინფორმაცია, მაგრამ თეორემა 1-ის თანახმად, ეს ზრდის ბიტების რაოდენობას, რომელთა დისტილაციაც ნებისმიერს შეუძლია. ამას ზოგჯერ ცოდნის გაფუჭებას უწოდებენ და ართულებს SKD პროტოკოლის ოპტიმიზაციას და ბიტების რაოდენობის გამოთვლას, რომლის მიღებაც რეალურად შესაძლებელია.

3.4 კონფიდენციალურობის გაძლიერება ექსტრაქტორების საშუალებით

უხეშად რომ ვთქვათ, ექსტრაქტორი არის ფუნქცია, რომელიც იღებს ერთგვაროვნად შემთხვევით ბიტებს სუსტი შემთხვევითი წყაროდან დამატებითი შემთხვევითი ბიტების მცირე რაოდენობის მეშვეობით, რომელიც გამოიყენება, როგორც კატალიზატორი . ექსტრაქტორები პირველად განსაზღვრა ნისანმა და ცუკერმანმა თეორიული კომპიუტერული მეცნიერების კონტექსტში. მათ გააჩნიათ სირთულის ანალიზის და პროტოკოლის მრავალფეროვანი აპლიკაცია, კერძოდ, ისინი იძლევა შემთხვევითი ალგორითმების სიმულაციის საშუალებას, მაშინაც კი როდესაც შემთხვევითობის მხოლოდ სუსტი წყაროებია ხელმისაწვდომი.

განმარტება 3. დავუშვათ $U^{(t)}$ არის შემთხვევითი ცვლადი ერთგვაროვანი განაწილებით $\{0,1\}^t$ -ზე. ფუნქციას $EN: \{0,1\}^{ln} \times \{0,1\}^{ht} \to \{0,1\}^k$ ეწოდება (δ, ϵ)- ექსტრაქტორი, თუ რომელიმე ცვლადისთვის X მწკრივით $\{0,1\}^{ln}$ და მინიმალური ენტროპიით $HF_\infty(X) \geq \delta l$, ვარიაციული მანძილი $\left[U^{(ht)}, \mathrm{EN}(\mathrm{X}, U^{(ht)})\right]$ და $U^{(ht+k)}$ განაწილებას შორის არის მაქსიმუმ ϵ. ვარიაციული მანძილი ორ განაწილებას HP_1 და HP_2 შორის იმავე მწკრივზე განისაზღვრება როგორც $\sum_{\mathrm{x}} |\mathrm{HP}_1(\mathrm{x}) - \mathrm{HP}_2(\mathrm{x})|/2.$).

კვლავ მიგვაჩნია, რომ კლოდმა და დომინიკმა განახორციელეს რეკონსილიაცია და შესაბამისად შეთანხმდნენ საერთო ცვლადზე, რომელიც აქ აღინიშნება X -ით. მაურერმა და ვულფმა აჩვენეს, რომ შესაძლებელია

ექსტრაქტორების გამოყენება კონფიდენციალურობის გაძლიერების განსახორციელებლად.

თეორემა 2. დავუშვათ δ, Δ_1, $\Delta_2 > 0$ წარმოადგენს კონსტანტებს. საკმარისად დიდი LN-თვის, დავუშვათ $HP_{XZ'}$ არის თავისუფალი ალბათობის განაწილება X -ის დამატებით $\{0,1\}^l$ - ში. დავუშვათ z' არის Z' -ის კონკრეტული სიდიდე, რომელიც შესწავლილია ევას მიერ, ისე რომ ევას მინ- ენტროპია $HF_\infty(X|Z' = z')$, X -ის შესახებ ცნობილია, რომ არის სულ მცირე δl. მაშინ იმოქმედებს ფუნქცია: $E : \{0,1\}^{lh} \times \{0,1\}^t \to \{0,1\}^k$, t -ით, $\leq \Delta_1 \mathrm{LH}$ და $k \geq (\delta - \Delta_2)lh$, ისე რომ როდესაც კლოდი და დომინიკი აირჩევენ $K = E(X,U)$ თავიანთ საიდუმლო გასაღებად, სადაც U არის შემთხვევითად და ერთგვაროვნად შერჩეული ბიტი, ისინი მიიღებენ შემდეგს

$$HF(K \mid U, Z' = z') \geq k - 2^{-lh^{1/2-o(1)}} \qquad (33)$$

რაც შეეხება კონფიდენციალურობის გაძლიერებას ჰეშ ფუნქციებით, ექსტრაქტორს შეუძლია ევას გაურკვევლობის გაზრდა, ისე რომ საბოლოო გასაღები K ვირტუალურად ფარული იყოს. თუმცა არის რამდენიმე განსხვავებაც. პირველი, მოსმენილი ინფორმაცია ამჯერად უნდა განისაზღვროს მინ - ენტროპიის გათვალისწინებით order-2 რენი ენტროპიის ნაცვლად. კიდევ ერთი განსხვავება ისაა, რომ ფუნქციაში შესასვლელი (U) შემთხვევითი ბიტების რაოდენობა შეიძლება გაცილებით დაბალი იყოს ექსტრაქტორებისთვის ვიდრე ჰეშ ფუნქციებისთვის. ეს შეიძლება გამოსადეგი იყოს გარკვეულ გარემოებებში, მაგალითად, როდესაც ხდება ამ თეორემების გამოყენება დასაკავშირებელი არხისთვის. დაბოლოს, თეორემა 2 ამტკიცებს ასეთი ექსტრაქტორების არსებობას საკმარისად დიდი შესასვლელი სიდიდეებით, მაგრამ არ იძლევა მათი არსებობის გარანტიას ყველა პარამეტრის სიდიდესთვის.

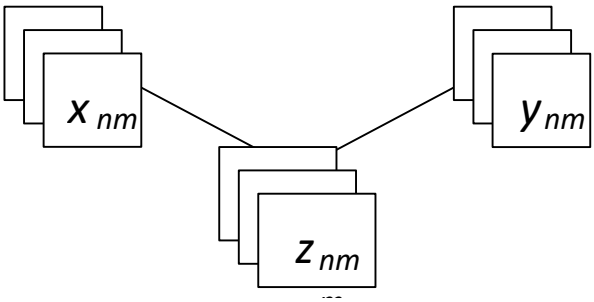
ბოლო შენიშვნის სახით, გაითვალისწინეთ, რომ მხედველობაში უნდა მივიღოთ რეკონსილიაციის შესახებ ინფორმაციის ცოდნა. ჰეშ ფუნქციებით კონფიდენციალურობის გაძლიერების მსგავსად, რომ

$$HF_\infty(X|Z' = zm) \geq H_\infty(X|Z = z) - |Mes| - \mathrm{h}s \qquad (33)$$

$1 - 2^{-hs}$ ალბათობით.

3.5 აუთენტიფიცირებული საიდუმლო გასაღების განმეორებითი დისტილაცია

ამ ნაწილში განვიხილავთ აუთენტიფიცირებული SKD -ის შემთხვევას დისკრეტული შემთხვევითი ცვლადების X, Y და Z მრავალჯერადი შედეგებიდან გამომდინარე, რომელიც ილუსტრირებულია ნახაზზე 10. ცალ - ცალკე განვიხილავთ ცალმხრივ და ორმხრივ კომუნიკაციებს.



ნახაზი 10. განმეორებითი დისტილაცია.

განმეორებით ასპექტში, კლოდს, დომინიკს და ევას წვდომა აქვთ შემთხვევითი ცვლადების X, Y და Z მრავალ შედეგზე.

3.6 ცალმხრივი კომუნიკაციები

ცალმხრივი კომუნიკაციების საშუალებით, ვთვლით, რომ კლოდი არის ის პირი, რომელიც ინფორმაციას უგზავნის დომინიკს. შედეგად, უნდა ვივარაუდოთ, რომ გასაღები წარმოადგენს კლოდის K = K(X) ცვლადის ფუნქციას.

ფორმალურად, Y და Z ცვლადები შეიძლება ჩაითვალოს, როგორც X -ის გაგზავნის შედეგი დასაკავშირებელი არხის საშუალებით, რომელიც ხასიათდება პირობითი ერთობლივი განაწილებით $HP_{Y\ z|X}$. შემდეგ პრობლემა ეხება საიდუმლო ბიტების რაოდენობის განსაზღვრას, რომელიც კლოდს შეუძლია გაუგზავნოს დომინიკს, რომელიც განისაზღვრება როგორც შესაბამისი დასაკავშირებელი არხის ფარული მოცულობა. ფარული მოცულობის თავდაპირველი განმარტება უზრუნველყო ვაინერმა, რომელმაც განიხილა შემთხვევა, სადაც ევას შეუძლია მოსმენა მხოლოდ არხის გამოსასვლელზე (დომინიკის მიერ მიღებული სიდიდე) დამატებითი დამოუკიდებელი არხის საშუალებით.

3.7 აუთენტიფიცირებული საიდუმლო გასაღების განმეორებითი დისტილაცია

ცსისზარმა და კორნერმა შემდეგ მოახდინეს ვაინერის შემოქმედების გენერალიზება იმის გათვალისწინებით, რომ მოსმენა შეიძლება განხორციელდეს წყაროს მხრიდან.

განმარტება 4. უმეხსიერებო დასაკავშირებელი არხის ძლიერი ფარული მოცულობა $\bar{C}_S(P_{YZ|X})$, რომელიც ხასიათდება პირობითი ერთობლივი განაწილებით $P_{YZ|X}$ წარმოადგენს მაქსიმუმ კოეფიციენტს $R \geq 0$ ისე რომ $\forall \epsilon > 0$ არსებობს $l > 0$ (ალბათური) დაშიფვრის ფუნქცია: $\{0,1\}^k \rightarrow X^{LN}$, და (ალბათური) გაშიფვრის ფუნქცია $d : Y^{LN} \rightarrow \{0,1\}^k$, $k = \lfloor (R - \epsilon)LN \rfloor$ -თან ერთად და X (ან Y), X (ან Y) -ის დამატებითი ფუნქცია, ისე რომ K -ს შემთხვევაში, რომელიც ერთგვაროვნად ნაწილდება $\{0,1\}^k$ -ზე, და $X_{1\ldots LN} = \epsilon(K)$ და $K' = hd(Y_{1\ldots LN})$ -ის შემთხვევებისთვის, ჩვენ გვაქვს $HPr[K \neq K'] \leq \epsilon$ და $H(K|_{Z1\ldots LN}) > k\,\epsilon$.

გაითვალისწინეთ, რომ თავდაპირველ განმარტებას, რომელიც აღინიშნება $C_S(P_{YZ|X})$ აქვს შედარებით სუსტი მოთხოვნები ფარულობასთან დაკავშირებით. მიუხედავად ამისა, მაურერმა და ვულფმა აჩვენეს , რომ $\bar{C}_S(HP_{YZ|X})= C_S(HP_{YZ|X})$, შესაბამისად, ჩვენ ჩავიჭრებით. ფარული მოცულობა განისაზღვრება შემდეგნაირად:თეორემა 3 $C_S(HP_{YZ|X}) = \max_{P_{UX}}[IN(U;Y) - IN(U;Z)]$, სადაც H$P_{UXYZ}$=H$P_{UX}P_{YZ|X}$. *იმ შემთხვევაში თუ IN(X;Y) ≥ IN(X;Z),* P_X -ის ყველა ალტერნატივისთვის,მაშინ

$$C_S(P_{YZ|X}) = \max_{HP_X}[IN(X;Y) - IN(X;Z)] \qquad (34)$$

-ის ალბათობებზე მაქსიმიზაციას განიხილავენ ცისისზარი და კორნერი, ვინაიდან ისინი იკვლევენ დამაკავშირებელ არხს. იმ შემთხვევაში როცა X -ის ალბათობა ფიქსირებულია (მაგალითად, დადგენილია შერჩეული QKD პროტოკოლის მოდულაციით), მაქსიმიზაცია უნდა განხორციელდეს მხოლოდ U-ზე, საჭიროების შემთხვევაში. კერძოდ, თეორემა 3 გულისხმობს, რომ პიროვნებას შეუძლია მოახდინოს IN(X;Y)–IN(X;Z) საიდუმლო გასაღების ბიტების დისტილაცია ასიმპტომურად დიდი ბლოკური კოდების გამოყენებით. ამ თეორემის თავდაპირველი დამტკიცება დაფუძნებულია შემთხვევითი კოდირების არგუმენტებზე. საინტერესოა, რომ დამტკიცება ძლიერი ფარულობის მოცულობაზე დამყარებულია ექსტრაქტორებზე.

3.8 ორმხრივი კომუნიკაციები

როდესაც დაშვებულია ორმხრივი კომუნიკაცია, დომინიკს შეუძლია კლოდს დაუბრუნოს გარკვეული ინფორმაცია. ამ შემთხვევაში, პირი უნდა გასცდეს დასაკავშირებელი არხის ცნებას, რადგან საბოლოო გასაღები შეიძლება დამოკიდებული იყოს ორივე ცვლადზე X და Y. ახლა განვიხილავთ შემთხვევას, როცა კლოდი და დომინიკი მუშაობენ წინასწარგანსაზღვრული პროტოკოლით, რომლის დროსაც შეტყობინებები შედის ორივე მიმართულებით. პროტოკოლის ბოლოს, ორივე ლეგიტიმურმა მხარემ უნდა შეძლოს განსაზღვროს K_C and K_D, რომელიც თავისუფალი მაღალი ალბათობის ტოლია და რომლებიც მოიცავს თავისუფალ საიდუმლო ბიტებს.

მოცემული ერთობლივი განაწილებისთვის HP_{XYZ}, ფორმალურად განისაზღვრება საიდუმლო გასაღების კოეფიციენტი, რომელიც მომდევნო განმარტებაშია ნაჩვენები.

განმარტება 5. X და Y -ის ძლიერი საიდუმლო გასაღების კოეფიციენტი Z-თან მიმართებაში, რომელიც აღინიშნება $\bar{S}(X; Y \parallel Z)$ -ით, არის მაქსიმალური კოეფიციენტი $R \geq 0$, ისე რომ $\forall \epsilon > 0$ და $\forall LN \geq N_0(\epsilon)$ არსებობს ცვლადი K, K -ს მწკრივით და პროტოკოლით, საჯარო კომუნიკაციების გამოყენებით არასაიმედო მაგრამ აუთენტიფიცირებულ არხზე, რომლის დროსაც ცვლადების l დამოუკიდებელი ნიმუშები ეძლევა: $X_{1\ldots LN}$ კლოდს, $Y_{1\ldots LN}$ დომინიკს და $Z_{1\ldots LN}$ ევას, ისე რომ კლოდს და დომინიკს შეუძლია გამოითვალონ გასაღებები K_C და K_D შესაბამისად, რაც ადასტურებს $HPr[KHC = K \wedge KD = K] \geq 1 - \epsilon$, $I(K;Z_{1\ldots LN}Mes) \leq \epsilon$ და $HF(K) = \log|K| \geq LN(R - \epsilon)$ ამ ფორმულას კლოდისა და დომინიკის მიერ გაგზავნილი Mes შეტყობინებების ერთობლიობა არასაიმედო არხზე.

გაითვალისწინეთ, რომ მაურერის მიერ მოცემულ თავდაპირველ განმარტებას, რომელიც აღნიშნულია HS(X;Y k Z) -ით, აქვს შედარებით სუსტი ფარულობის მოთხოვნები. თუმცა, მაურერმა და ვულფმა აჩვენეს, რომ $HS^{-}(X;Y \text{ k } Z) = HS(X;Y \text{ k } Z)$, შესაბამისად ჩვენ ისევ ჩავიჭრებით. HS(X;Y k Z) -ის დახურული ფორმა უცნობია და ზედა და ქვედა ზღვრები მოცემულია 4 და 5 თეორემებში.

თეორემა 4. საიდუმლო გასაღების კოეფიციენტი HS(X;Y k Z) ქვედა - ზღვრით ფასდება შემდეგნაირად

$$HI(X;Y) - \min[HI(X;Z), HI(Y;Z)] \leq HS(X;Y \text{ k } Z). \quad (35)$$

საინტერესოა აღინიშნოს, რომ 4 თეორემაში არსებული ქვედა ზღვარი დაფუძნებულია 1 თეორემაზე. X, Y და Z -ის ნიმუშების მაღალი რიცხვების შემთხვევაში, ასიმპტომური თანაბარი განაწილება ამტკიცებს, რომ უმეტესად $X^{(LN)}$, $Y^{(LN)}$ და $Z^{(LN)}$ მიეკუთვნება ჩვეულებრივი მიმდევრობის სიმრავლეს, რომლებიც ერთგვაროვნად ნაწილდება. გამომდინარე ჩვეულებრივი $X^{(LN)}Y^{(LN)}Z^{(LN)}$ -დან (რომლის ალბათობა შეიძლება

თავისუფლად მაღალი იყოს), რენის ენტროპია შეესაბამება შენონის ენტროპიას. ეს საშუალებას გვაძლევს ვთქვათ, რომ მისაღები საიდუმლო ბიტების რაოდენობა წარმოადგენს სულ მცირე კლოდის HF(X) მიერ წარმოებული ბიტების რაოდენობას, რომელიც დაყვანილ იქნა დომინიკისთვის გამოვლენილ X, კერძოდ HF(X|Y) ბიტების რაოდენობაზე და იმ ბიტების რაოდენობაზე IN(X;Z), რომელიც ევასთვის გახდა ცნობილი, აქედან გამომდინარე

$HF(X) - HF(X|Y) - IN(X;Z) = IN(X;Y) - IN(X;Z)$.

რა თქმა უნდა, იგივე არგუმენტი მოქმედებს თუ გასაღები ეფუძნება დომინიკის ბიტებს, აქედან გამომდინარე HI(X;Y) – HI(Y ;Z) ასევე დასაშვებია.

HS(X;Y k Z) -ის პირველი ზედა ზღვარი მოცემულ იქნა მაურერის მიერ, კერძოდ

HS(X;Y k Z) ≤ min[I(X;Y),I(X;Y |Z)].

3.9 აუთენტიფიცირებული საიდუმლო გასაღების განმეორებითი დისტილაცია

ეს ინსტიქტურად შეიძლება აიხსნას იმ ფაქტით, რომ საიდუმლო ბიტების რაოდენობა, რომლის დისტილაციაც კლოდს და დომინიკს შეუძლია, არ შეიძლება აღემატებოდეს ბიტების რაოდენობას რომლებსაც ისინი იზიარებენ აპრიორი ან ბიტების იმ რაოდენობას, რომლებსაც იზიარებენ ევას მიერ Z -ის შესახებ ინფორმაციის ცოდნის მიღმა. შემდეგ, მაურერმა და ვულფმა შეიმუშავეს შიდა ორმხრივი მონაცემების ცნება (intrinsic mutual information) რათა გაეუმჯობესებინათ ზედა ზღვარი. ექსპერიმენტის სახით, ზემოხსენებული ზედა ზღვარი ასევე მოქმედია ნებისმიერი Z-ცვლადისთვის, რომელიც მიიღება Z -ის გაგზავნით თავისუფალი არხის საშუალებით. X და Y-ს შორის მოცემული Z-ით არის

$$\mathrm{HI}(\mathrm{X};\mathrm{Y}\downarrow\mathrm{Z}) = \inf_{\mathrm{P}_{\bar{\mathrm{Z}}|\mathrm{Z}}} \mathrm{HI}(\mathrm{X};\mathrm{Y}\mid\bar{\mathrm{Z}}), \qquad (36)$$

PXY ZZ =PXYZP Z|Z -ით. მაშინ, ჩვენ ვიღებთ ზედა ზღვარს $HS(X;Y \parallel Z) \leq \mathrm{HI}(X;Y\downarrow Z)$. საბოლოოდ $HS(X;Y \parallel Z)$-ის ზედა ზღვარი განავრცო რენერმა და ვულფმა იმის გათვალისწინებით, რომ თუ ევას ეცოდინება დამატებითი ცვლადი Z_{extra} , ჩვენ მივიღებთ $HS(X;Y \parallel Z) \leq \mathrm{H}S(X;Y \parallel ZZ_{\text{extra}}) + HF(Z_{\text{extra}})$. საიდუმლო გასაღების კოეფიციენტი შემდეგ შემცირდება ყველა ასეთი შესაძლო დამატებითი ცვლადების გამოყენებით. შემცირებული *შიდა ორმხრივი მონაცემები* X და Y-ს შორის, მოცემული Z -ით არის

$$HI(X;Y\downarrow\downarrow Z) = \inf_{P_{Z_{\text{extral}}\,XYZ}} \left(HI(X;Y\downarrow ZZ_{\text{extra}}) + HF(Z_{\text{extra}})\right). \qquad (37)$$

თეორემა 5. საიდუმლო გასაღების კოეფიციენტი $\mathrm{H}S(X;Y\mathrm{k}\,Z)$ ზედა ზღვარზე შეფასებულია, როგორც $HS(X;Y\mathrm{k}\,Z) \leq IN(X;Y\downarrow\downarrow Z)$. აღნიშნულის წერის დროს, 5 თეორემაზე შეზღუდული ზღვრები ცნობილი არაა. პრაქტიკაში, ორმხრივი კომუნიკაციების საშუალებით საიდუმლო გასაღების დისტილაციის შედეგები მარტივი გამოსაყენებელი არაა. ორ ეტაპიანი მიდგომის გამოყენებისას, კერძოდ რეკონსილიაციისას, რომელიც მოიცავს კონფიდენციალურობის გაძლიერებას, უნდა შემოვიფარგლოთ აღნიშნული ზღვარით IN(X;Y) – min[HI(X;Z),HI(Y ;Z)]. ვინაიდან პრაქტიკული კოდირების მეთოდები არ აკმაყოფილებს შენონის ენტროპიებს, პრაქტიკული შედეგი უფრო პესიმისტურია, კერძოდ

$$HS_{\text{practical}} < IN(X;Y) - \min[I(X;Z),I(Y;Z)]. \qquad (38)$$

პრინციპში, ორმხრივი კომუნიკაციები საშუალებას აძლევს პირს დაძლიოს ეს ფორმულა. მაგალითად, განვიხილოთ სამი ორმაგი შემთხვევითი ცვლადის X, Y და Z, შემთხვევა X = Y = Y = {0,1} -თან ერთად. თითოეული ეს ცვლადი დაბალანსებულია, ანუ $HP_X(0) = HP_X(1) = HP_Y(0) = HP_Y(1) = HP_Z(0) = HP_Z(1) = 1/2$.

ისინი დაკავშირებულია წყვილებად, მაგრამ არა სრულყოფილად: $\mathrm{HPr}[X = Y] = 1 - \epsilon_{XY}$, $\mathrm{HPr}[Y = Z] = 1 - \epsilon_{YZ}$ და $\mathrm{HPr}[Z = X] = 1 - \epsilon_{ZX}$, ზოგიერთი რეალური

სიდიდისთვის $0 < \epsilon_{XY}, \epsilon_{YZ}, \epsilon_{ZX} \leq 1/2$. მაურერმა აჩვენა, რომ $\epsilon_{XY} > \epsilon_{ZX}$ და $\epsilon_{XY} > \epsilon_{YZ}$ -ის შემთხვევაშიც კი, შესაძლებელია საიდუმლო გასაღების დისტილაცია ორმხრივი კომუნიკაციების საშუალებით. ან სხვაგვარად რომ ვთქვათ, არა - ნულოვანი საიდუმლო გასაღების კოეფიციენტი დასაშვებია ამ შემთხვევაშიც კი $IN(X;Z) > IN(X;Y)$ და $IN(Y;Z) > IN(X;Y)$. მიუხედავად ამისა, ასეთი მხოლოდ ერთი შემთხვევაა და სამწუხაროდ, არც ერთი უნივერსალური ფორმულა არ არის ცნობილი.

3.10 არა აუთენტიფიცირებული საიდუმლო გასაღების დისტილაცია

აქამდის განვიხილეთ შემთხვევა, რომლის დროსაც ღია (საჯარო) არხი აუთენტიფიცირებულია დისტილაციის პროტოკოლის მიღმა. ამ ნაწილში, ჩვენ განვიხილავთ და წარმოვადგენთ შედეგებს იმ შემთხვევის შესახებ, რომლის დროსაც აუთენტიფიკაცია არ არის ნავარაუდები და აქტიური მტრებისგან დაცვა უზრუნველყოფილი უნდა იყოს როგორც თვით დისტილაციის პროტოკოლის ნაწილი.

აქტიურ მტერთან პირდაპირ გამკლავების იდეა, საიდუმლო გასაღების დისტილაციის ფარგლებში პირველად გამოიკვლია მაურერმა. მისი კვლევა შემდეგ გენერალიზდა ვულფთან ერთად და მათი ერთობლივი შედეგები გამოქვეყნდა სამ ნაშრომად: რომელიც განიხილავს ზოგად შედეგებს და განმეორებით არა - აუთენტიფიცირებულ SKD -ს, რაც წარმოადგენს ახალ საშუალებას იმის განსასაზღვრად არის თუ არა ეს ორი განაწილება იმიტირებული (იხილეთ განმარტება 7) რომელიც წარმოადგენს შედეგებს კონფიდენციალურობის გაძლიერებასთან დაკავშირებით ჰეშ ფუნქციების უნივერსალური ოჯახებით და ერთჯერადი არა - აუთენტიფიცირებული SKD ექსტრაქტორებით. ამჯერად ჩვენ აქცენტს გავაკეთებთ განმეორებით შედეგებზე. საიდუმლო გასაღების კოეფიციენტი მორგებულია არა-აუთენტიფიცირებულ შემთხვევაზე, შემდეგნაირად.

განმარტება 6. *X და Y -ის ძლიერი საიდუმლო გასაღების კოეფიციენტი Z -თან მიმართებაში, რომელიც აღნიშნულია $HS^*(X;Y\|Z)$ -ით, მოიცავს იგივე განმარტებას, როგორსაც განმარტება 5 იმ მოდიფიკაციით, რომ კლოდს და დომინიკს შორის არსებული არხი არ არის აუთენტიფიცირებული და რომ ნებისმიერი $\delta > 0$ -ის შემთხვევისთვის, რომელსაც გააჩნია $1 - \delta$ ალბათობა, ორივე მხარე უარყოფს პროტოკოლს (თუ ევა შეცვლის კლოდსა და დომინიკს შორის არსებულ შეტყობინებებს) ან პროტოკოლი წარმატებულია.*

მთავარ შედეგში ნათქვამია, რომ თუ ევა როგორმე შეძლებს კლოდის (ან დომინიკის) მიბაძვას, იგი არ იქნება განსხვავებული კლოდისგან (ან დომინიკისგან) მეორე მხარისთვის. უფრო ფორმალურად რომ ვთქვათ, შეუძლია თუ არა ევას მიბაძოს რომელიმე მხარეს განისაზღვრება ერთობლივი ალბათობის განაწილებით $HP_{XY\,Z}$. მოცემული Z -ით მას შეიძლება ჰქონდეს შესაძლებლობა წარმოქმნას ახალი შემთხვევითი ცვლადები, ისე რომ შეძლოს X ან Y -ის სიმულაცია. ეს მდგომარეობა გამოხატულია მე-7 განმარტებაში.

განმარტება 7. შემთხვევითი ცვლადი X -ის სიმულაცია ხდება Z -ით Y -თან მიმართებაში, რომელიც აღინიშნება $\mathrm{sim}_Y(Z \to X)$, თუ არსებობს პირობითი განაწილება $P_{\bar{X}|Z}$ ისე რომ $HP_{\bar{X}Y} = HP_{XY}$

თეორემა 6. ძლიერი საიდუმლო გასაღების კოეფიციენტი $\mathrm{HS}^*(X;Y\|Z)$ ტოლია $\mathrm{HS}^*(X;Y\|Z) = \mathrm{HS}(X;Y\|Z)$ საიდუმლო გასაღების კოეფიციენტისა, იმ შემთხვევაში თუ არ არის $\mathrm{sim}_Y(Z \to X)$ ან $\mathrm{sim}_X(Z \to Y)$, რომელ შემთხვევაშიც $\mathrm{HS}^*(X;Y\|Z)=0$.

თეორემა 6 -ში აღნიშნულია, რომ თუ ევას შეუძლია მოახდინოს X ან Y -ის სიმულაცია, მაშინ დისტილაცია ვერ მოხერხდება: კლოდმა (ან დომინიკმა) შეიძლება ვერ შეძლოს განასხვაოს დომინიკი (ან კლოდი) ევასგან.

თეორემა 6 ასევე აღნიშნავს, რომ თუ ევა ვერ შეძლებს მიბაძოს რომელიმე მხარეს, ამ შემთხვევაში SKD მოქმედებს და საკმაოდ კარგი პროტოკოლიდან გამომდინარე, საიდუმლო გასაღების კოეფიციენტი არ უშვებს იმ ფაქტს, რომ ასევე აქტიური მტრები უნდა იქნას მხედველობაში მიღებული. მაგრამ

ნიშნავს თუ არა ეს იმას, რომ ჩვენ არ გვჭირდება საიდუმლო გასაღები დასაწყებად? უნდა გამოვრიცხოთ რაც 5.1.1 ნაწილშია ნათქვამი? როგორც ახლა განვიხილავთ, პასუხი უარყოფითია: QKD -ის მიხედვით, კლოდს და დომინიკს მაინც სჭირდებათ (მოკლე) საიდუმლო გასაღები დასაწყებად. საიდუმლო გასაღების დისტილაციისთვის საფასურის გადახდა საწყისი ჩატვირთვის საიდუმლო გასაღების გარეშე წარმოადგენს ერთობლივი ალბათობის განაწილების მეცნიერებას HP_{XYZ}. კლოდის (ან დომინიკის) თვალსაზრისით, იმის ცოდნა თუ რა სტატისტიკური განსხვავებებია Y (ან X) და Z -ს შორის მნიშვნელოვანია და წარმოადგენს თეორიას, რომელიც გათვალისწინებულ უნდა იქნას. ან სხვაგვარად, რომ ვთქვათ HP_{XYZ}-ის ცნება გარკვეულწილად კლოდის და დომინიკის საერთო საწყისი ჩატვირთვის საიდუმლო გასაღების ტოლია. QKD -ში, ერთობლივი ალბათობის განაწილება HP_{XYZ} წინასწარ არ არის ცნობილი, მაგრამ უნდა გამოითვალოს. ამ გამოთვლის დროს, კლოდი და დომინიკი ცვლიან X და Y ცვლადების ქვეჯგუფს. აღნიშნული გაცვლა არ არის საჭირო იყოს ფარული, რადგან იხარჯება გაცვლილი გასაღების ელემენტები და არ წარმოდგენს საბოლოო გასაღების ნაწილს, თუმცა მას სჭირდება აუთენტიფიცირება. პროტოკოლის ამ ნაწილის აუთენტიფიკაციის არარსებობის შემთხვევაში, კლოდს (ან დომინიკს) არ შეეძლება განასხვავოს დომინიკი (ან კლოდი) და ევა, რაც ნიშნავს, რომ აქტიურ მტერს შეეძლება დაამონტაჟოს შეტევა შუაგულში. ბოლო შენიშვნის სახით, უნდა ავღნიშნოთ, რომ ორმხრივი მონაცემების სიდიდეების IN(X;Y), IN(X;Z) და IN(Y ;Z) ცოდნა არ არის ყოველთვის საკმარისი სიმულაციური მდგომარეობების განსასაზღვრად. კერძოდ, HP_{XY}-დან გამომდინარე, თუ $IN(X;Y) \leq IN(X;Z)$ *(ან თუ* $IN(X;Y) \leq IN(Y;Z)$*)* მაშინ ყოველთვის იარსებებს შემთხვევითი ცვლადი Z, რომელიც აკმაყოფილებს განსაზღვრულ ორმხრივი მონაცემების სიდიდეებს, ისე რომ

$$\mathrm{sim}_Y(Z \to X) \text{ (or } \mathrm{sim}_X(Z \to Y)). \qquad (39)$$

3.11 საიდუმლო გასაღების დისტილაცია უწყვეტი ცვლადებით

ზემოთ მოცემულ ნაწილებში, კლოდის და დომინიკის ცვლადები X და Y ითვლება დისკრეტულად. ამჯერად განვიხილავთ როგორ ხდება საიდუმლო გასაღების დისტილაცია როცა X და Y უწყვეტია.

მნიშვნელოვანი დეტალი, რომელიც უნდა აღინიშნოს არის დისტილაციის პროტოკოლის თუ რომელი ნაწილები უნდა იყოს დისკრეტული ან უწყვეტი. კერძოდ, ჩვენ უნდა განვიხილოთ შემდეგი შეკითხვები: „საჭიროა თუ არა საბოლოო გასაღებიც იყოს უწყვეტი? და რა აზრის ხართ რეკონსილიაციის (შეთანხმების) შეტყობინებებზე?“ სინამდვილეში, მე გიჩვენებთ, რომ ორივე, საბოლოო გასაღები და რეკონსილიაციის შეტყობინებები უნდა იყოს დისკრეტული, მაშინაც კი თუ გასაღების ელემენტები უწყვეტია. პირველი, უწყვეტ საიდუმლო გასაღებს მარტივად რომ ვთქვათ დიდი მნიშვნელობა არ აქვს პრაქტიკაში. იგი გამოყენებულ უნდა იქნას ერთჯერადი ბლოკნოტის უწყვეტ ვარიანტთან ერთად, რაც შესაძლებელია, მაგრამ ამავდროულად რთულია გახდეს ხმაურისადმი რეზისტენტული. საკმაოდ მოუხერხებელია შეცდომების ვარიაციების გადაჭრა რეალურ რიცხვებზე, რადგან ნებისმიერი რესურსით - შეზღუდულ დამუშავებას შეუძლია მხოლოდ შეცდომების უფრო მეტად გავრცელება. გარდა ამისა, არ არსებობს პრაქტიკულად გამოსადეგი უწყვეტი ერთჯერადი ბლოკნოტი. არსებობს სხვა უწყვეტი დაშიფვრის სქემები, მაგრამ მათი უსაფრთხოება არ არის საკმარისი QKD -ის კონტექსტში. მაგალითად, არსებობს ხმის არევის მეთოდები, რომელიც ამუშავებს ანალოგიურ სიგნალებს, თუმცა ვერ უზრუნველყოფს სრულ ფარულობას. კიდევ ერთი მაგალითია სინქრონულ ქაოსზე დაფუძნებული კრიპტოგრაფია. ამ შემთხვევაში, დაშიფრული სიგნალი უბრალოდ ემატება გარკვეულ ქაოტურ ხმაურს. უსაფრთხოება იმაში მდგომარეობს, რომ ხმაურს უფრო დიდი ამპლიტუდა აქვს ვიდრე მთელი სპექტრის სიგნალს. ისევ და ისევ, იგი უფრო სუსტია ვიდრე სრული ფარულობა.

მეორე, რეკონსილიაციის შეტყობინებები შეიძლება იყოს უწყვეტი ან დისკრეტული. თუ ღია (საჯარო) აუთენტიფიცირებულ კლასიკურ არხს არ აქვს უსრული მოცულობა, გაცვლილი რეკონსილიაციის შეტყობინებები ან დისკრეტულია ან ხმაურიანი უწყვეტი სიდიდეები. ამ უკანასკნელ შემთხვევას დამატებითი გაურკვევლობები შეაქვს პროტოკოლში, რაც ჩვენს მიზნებს ეწინააღმდეგება. მაგალითად, კონფიდენციალურობის გაძლიერების პროტოკოლი (მაგ.: ჰეშ ფუნქციებზე დაფუძნებული) გამიზნულია მთლიან გასაღებზე გაავრცელოს გაურკვევლობა, მისი წარმოშობისგან დამოუკიდებლად. ამრიგად, გაცვლილ შეტყობინებებში ხმაური ისევე გავრცელდება როგორც ვრცელდება ევას გაურკვევლობა. დაბოლოს, ხმაურიანი უწყვეტი რეკონსილიაციის შეტყობინება უფრო ნაკლებ ეფექტურ სარგებელს მიიღებს კლასიკური არხის აუთენტიფიკაციის მახასიათებლიდან. აუთენტიფიკაციის პროტოკოლს ძალიან გაუჭირდება ხმაურის შეცნობა ხმაურის წინააღმდეგ არსებული აქტიური მოწინააღმდეგის გამო, რომელიც არსებობს შეტყობინებების შიგნით. აქედან გამომდინარე, ბევრად უმჯობესია დისკრეტული საბოლოო გასაღები და დისკრეტული რეკონსილიაციის შეტყობინებები.

3.12 დისკრეტული გასაღების კლასის დისტილაცია უწყვეტი ცვლადებიდან

ახლა განვიხილავთ პროტოკოლების HC კლასს, რომლებიც ახდენენ დისკრეტული საიდუმლო გასაღების დისტილაციას უწყვეტი ცვლადებისგან დისკრეტული შეტყობინებების გამოყენებით. თუ ჩვენ გადავიყვანთ X და Y ცვლადებს დისკრეტულ ცვლადებად, ვთქვათ $X' = T_{\mathrm{HC}}(X)$ და $Y' = T_{\mathrm{D}}(Y)$, სანამ მოხდება მათი დამუშავება, ჩვენ ვიღებთ პროტოკოლების hC' კლასს, რომელიც ნამდვილად შესულია $hC' \subseteq hC$ -ის წინა კლასში. ჩვენ შეგვიძლია წარმოგიდგინოთ, რომ ეს ორი კლასი სინამდვილეში თანაბარია. ეს ნიშნავს, რომ დისტილაციის ეფექტურობაზე არ არსებობს არავითარი ჯარიმა იმ მოთხოვნასთან დაკავშირებით, რომ X და Y გადაყვანილ იქნას X′ და Y′ -ად

რეკონსილიციამდე და კონფიდენციალურობის გაძლიერებამდე. დისტილაციის პროცესი შეიძლება დაჯამდეს $k = f_{hC}(x,m)$ და $k = f_D(y,m)$ ფუნქციებად, რათა წარმოქმნას გასაღები k, სადაც mes აღნიშნავს გაცვლილ შეტყობინებებს. ვინაიდან ორივე, k და m აღებულ უნდა იქნას თვლად სიმრავლეში, ამ ორივე ფუნქციათაგან თითოეული განსაზღვრავს სიდიდეების ქვეჯგუფის თვლად ოჯახს, რომელიც იგივე შედეგს იძლევა: $hS_{km} = \{x : f_{hC}(x,m) = k\}$ and $S_{kmes'} = \{y : f_{HD}(y,mes) = k\}$. ქვეჯგუფის დადგენა რომელშიც მდებარეობს x (ან y) წარმოადგენს ერთადერთ საინტერესო მონაცემებს და მათი გამოსახვა შესაძლებელია დისკრეტული ცვლადების გამოყენებით, მაშინ როცა აღნიშნულ ქვეჯგუფში არსებული სიდიდე არ ახდენს გავლენას შედეგზე და შეიძლება უბრალოდ ჩაითვალოს ხმაურად. ცხადია, რომ არსებობს დისკრეტიზაციის ფუნქციები T_C და T_D და დისკრეტული პროტოკოლი წარმოდგენილია მომდევნო ფუნქციებით:

f'_C და f'_D ისე რომ $f'_C(T_{hC}(x), mes) = f_{hC}(x, mes)$ და $f'_{nm}(T_D(y), mes) = f_{HD}(y, mes)$.

ასევე, დისკრეტული გარდაქმნა არ ადებს ფუნდამენტურ ზღვარს შედეგად მიღებულ ეფექტიანობას. შესაძლებელია, რომ IN(THC(X);TD(Y)) სურვილისამებრ დავაახლოვოთ IN(X;Y) -თან. მეორეს მხრივ, არც ერთ სრულად უწყვეტ პროტოკოლს (ანუ, როგორიცაა უწყვეტი შეტყობინებები ან უწყვეტი გასაღების შედეგი) არ უნდა ჰქონდეს იმის მოლოდინი, რომ კლოდი და დომინიკი გააზიარებენ თავდაპირველზე მეტ IN(X;Y) საიდუმლო ინფორმაციას. ამრიგად,HC'=HC.

და მაინც, თუ საიდუმლო გასაღების დისტილაციამდე დისკრეტულ ცვლადებად გადაქცევა ისეთივე ეფექტურია, როგორც უწყვეტი დისტილაცია, რომელსაც მოჰყვება დისკრეტულ ცვლადებად გარდაქმნა, მაშინ რატომ იქნებოდა სასურველი პირველი მიდგომა? ამის მიზეზი არის ის, რომ რეალური ცვლადების დამუშავება შეცდომებისკენაა მიდრეკილი რეალისტური კომპიუტერის სასრული სიზუსტის გამო. რეალური სიდიდეების დამუშავება ასევე ნიშნავს ინფორმაციის ირელევანტური ნაწილების დამუშავებას (ანუ, ისინი, რომლებიც გავლენას არ ახდენენ

ზემოთ ხსენებულ ფუნქციებზე f_{HC} და f_{HD}), ამით ხდება რესურსების გაფლანგვა შესაბამისი ინფორმაციის რელევანტური ნაწილების სიზუსტის შემცირების ფასად. ზემოთ აღნიშნული ყველა მიზეზის გამო, საიდუმლო გასაღების ოპტიმალური დისტილაციის პროტოკოლი უნდა მოიცავდეს კლოდის და დომინიკის უწყვეტი ცვლადების გარდაქმნას დისკრეტულ ცვლადებად და დისკრეტული ინფორმაციის გაცვლას ორ საკომუნიკაციო მხარეს შორის, ისე რომ მოხდეს დისკრეტული საიდუმლო გასაღების დისტილაცია.

ამ თავში მიმოვიხილეთ საიდუმლო გასაღების დისტილაციის განსახორციელებელი სავარაუდო მეთოდები და მათთან დაკავშირებული თეორიული შედეგები. ასევე შევეხეთ უწყვეტი ცვლადების განსაკუთრებულ შემთხვევას.

ეფექტური საიდუმლო გასაღების დისტილაცია მნიშვნელოვანია QKD -ზე დაფუძნებული კრიპტოსისტემისთვის, იმ გაგებით, რომ კლოდმა და დომინიკმა უნდა მიაწოდონ საერთო საიდუმლო გასაღების ბიტების ოპტიმალური ოდენობა, ამავდროულად აკონტროლონ მათზე მოყურადის ცოდნის დონე. .

მომდევნო თავებში უფრო მეტად განვავრცობთ ამ თავში განხილული მეთოდების ქვეჯგუფს. კონკრეტულად, გასაგებად დავყოფთ SKD -ის რეკონსილიაციად და კონფიდენციალურობის გაძლიერებად. ზემოდან - ქვემოთ მიდგომის დაცვით, პირველ რიგში განვიხილავთ კონფიდენციალურობის გაძლიერებას ჰეშ ფუნქციების უნივერსალური ოჯახების გამოყენებით, რადგან ისინი საუკეთესოდ ფუნქციონირებს პრაქტიკაში. შემდეგ, განვიხილავთ რეკონსილიაციას, იმისათვის რომ გიჩვენოთ თუ როგორ შეუძლია ორ მხარეს რეალურად მიიღონ თანაბარი შუალედური გასაღებები.

თავი 4. კონფიდენციალურობის გაძლიერება ჰეშ ფუნქციათა უნივერსალური ოჯახების საშუალებით

ამ თავში განვიხილავთ ჰეშ ფუნქციების უნივერსალური ოჯახების რამდენიმე მნიშვნელოვან ასპექტს. სრულიად ზოგადი ინფორმაციით არ შემოვიფარგლებით, რადგან 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 მოვიყვანთ ოჯახთა შესახებ განმარტებებს და გიჩვენებთ თუ როგორ ერგება ისინი ჩვენს საჭიროებებს. დაბოლოს, განვიხილავთ მათ იმპლემენტაციას.

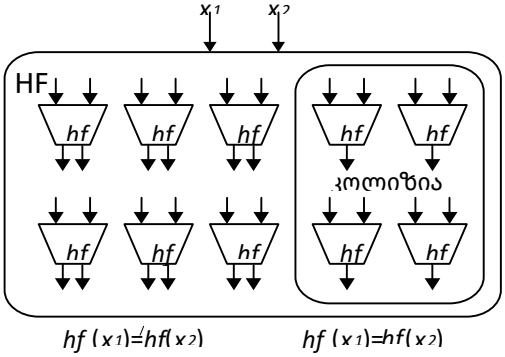
4.1 მოთხოვნები

კონფიდენციალურობის გაძლიერების მიზნით, ჰეშ ფუნქციების ოჯახები უნდა აკმაყოფილებდეს რამდენიმე მნიშვნელოვან მოთხოვნას. ისინი ჩამოთვლილია ქვემოთ:

- ოჯახი უნდა იყოს უნივერსალური ($\epsilon = 1$) ან მასთან ძალიან მიახლოებული ($\epsilon \approx 1$).
- კონკრეტული ჰეშ ფუნქციის ოჯახში მის წარმოსადგენად საჭირო ბიტების რაოდენობა უნდა იყოს ზომიერად დაბალი.
- ოჯახს უნდა გააჩნდეს დიდი შესასვლელი და დიდი გამოსასვლელი სიდიდეები.
- ჰეშ ფუნქციის შეფასება ოჯახში უნდა იყოს ეფექტური.

პირველი მოთხოვნა პირდაპირ ახდენს გავლენას წარმოქმნილი საიდუმლო გასაღების ხარისხზე. რაც უფრო ახლოსაა უნივერსალურობასთან, მით უკეთესია შედეგად მიღებული გასაღების ფარულობა.

მეორე მოთხოვნა გამომდინარეობს იქიდან, რომ ჰეშ ფუნქცია შემთხვევითად უნდა იქნას შერჩეული მის ოჯახში და მოცემული ალტერნატივა უნდა გადაიცეს კლოდსა და დომინიკს შორის. მიუხედავად ამისა, იგი არ არის კრიტიკული, რადგან ჰეშ ფუნქციის ალტერნატივა არ არის საჭირო, რომ ფარული იყოს. ბიტების რაოდენობა, რომელიც პროპორციულია შესასვლელის სიდიდესთან მისაღებია.



ნახაზი 11. მოთხოვნები

იმისათვის, რომ კონფიდენციალურობის გაძლიერებამ საუკეთესოდ იმუშაოს, ჰეშ ფუნქციათა ოჯახი უნდა იყოს ისეთი, რომ ნებისმიერი $x_1 \neq x_2$, ფუნქციათა სიმრავლე, რომელიც იძლევა იგივე გამოსასვლელს $hf(x_1) = hf(x_2)$ (ანუ, კოლიზია) უნდა იყოს რაც შეიძლება მცირე. რომ იყოს |HB|- ჰეშ ფუნქციის თითქმის უნივერსალური ოჯახი, შეიძლება არ წარმოშვას $\epsilon|HF|/|HB|$ კოლიზიაზე მეტი ნებისმიერი $x_1 \neq x_2$, |HF| ფუნქციათა რაოდენობისთვის ოჯახში და |HB| სიდიდის შესასვლელი სიმრავლისთვის. მოდით განვმარტოთ დიდი შესასვლელი და გამოსასვლელი სიდიდეების საჭიროება. QKD -ში, კონფიდენციალურობის გაძლიერების საშუალებით ამოსაღები ბიტების რაოდენობის გამოთვლა სტატისტიკურად განისაზღვრება კლოდის და დომინიკის მიერ, რომლებიც ადარებენ ზოგიერთ ნიმუშს. ასეთი გამოთვლა უნდა იყენებდეს ტესტის ნიმუშებს, რომელიც შემთხვევითად და ერთგვაროვნად ვრცელდება QKD სვლის ბლოკზე, რაც წინააღმდეგ შემთხვევაში, დროზე დამოკიდებული მოსმენის არასწორად გამოთვლას გამოიწვევს. ტესტის ნიმუშების რაოდენობის გაზრდა აუმჯობესებს სტატისტიკურ გამოთვლას, მაგრამ მეორეს მხრივ, იგი

ასევე ამცირებს გასაღებისთვის ხელმისაწვდომი ნიმუშების რაოდენობას. იდეალური სიტუაცია იქნება დიდი ბლოკური სიდიდის ქონა, რომლიდანაც შესაძლებელია ტესტის ნიმუშების დიდი რაოდენობით მიღება, მაგრამ რომლის პროპორციაც ბლოკურ სიდიდეში არის ძალიან მცირე. გაცვლის მიზნით, ვეძებთ ოჯახებს რაც შეიძლება დიდი შესასვლელი სიდიდით და პროპორციულად დიდი გამოსასვლელი სიდიდით. მაგალითად, კონფიდენციალურობის გასაძლიერებლად გამოყენებულ ჰეშ ფუნქციებს შეუძლია დაამუშავოს 110 503 ბიტი შესასვლელის სახით და აწარმოოს გამოსასვლელი ბიტების მცირე რაოდენობა. ეს ბიტები მომდინარეობს დაახლოებით 55200 ან 36800 კვანტური ნიმუშის სიდიდის ბლოკიდან, იმისდა მიხედვით ორ ბიტს მივიღებთ თუ სამს თითოეული ნიმუშიდან. ოპტიკურმა იმპლემენტაციამ მოგვცა 60000 პულსის ბიძგი.
და ბოლოს, ჰეშ ფუნქციის შეფასების ეფექტურობა მაღალი პრაქტიკული მნიშვნელობისაა. QKD -ის რეალურ დროში მოხმარების შემთხვევაში, საიდუმლო გასაღების დისტილაციამ ძალიან ბევრი დრო არ უნდა წაიღოს. ჰეშ ფუნქციის შეფასება კრიტიკულ გზაზეა საიდუმლო გასაღების დისტილაციის სხვა ეტაპებთან ერთად. აუთენტიფიკაციისთვის გამოყენებული ოჯახების შესასვლელი და გამოსასვლელი სიდიდის მოთხოვნები სრულიად განსხვავდება კონფიდენციალურობის გაძლიერების მოთხოვნებისგან: აუთენტიფიკაციისთვის გამოსასვლელი სიდიდე საკმაოდ მცირეა და არ იზრდება ან იზრდება ნელა შესასვლელის სიდიდესთან ერთად, კონფიდენციალურობის გაძლიერების დროს, მიუხედავად ამისა, გამოსასვლელი სიდიდე შესასვლელი სიდიდის პროპორციულია. ლიტერატურაში შეგიძლიათ მოიძიოთ მრავალი ოჯახი, რომელიც აგებულია აუთენტიფიკაციის გათვალისწინებით და მასში მოცემული ცნობები ან UMAC -ის ფორმულა. სამწუხაროდ, ყველა ამ ოჯახს აქვს მცირე გამოსასვლელი სიდიდეები.

4.2 ოჯახების კომბინაცია და გავრცობა

ბუნებრივია დავსვათ კითხვა შეგვიძლია თუ არა ჰეშ ფუნქციების ახალი ოჯახების შექმნა არსებულთან კომბინაციით ან მათი გავრცობით. გარკვეულწილად პასუხი არის დადებითი; თუმცა, ამ მიმართულებით მიღებული შედეგები არ არის დამაკმაყოფილებელი, რადგან ისინი არ აკმაყოფილებენ ჩვენს მოთხოვნებს.

პირველ რიგში, დავუშვათ ვყოფთ შესასვლელ x -ს ორ ნაწილად $x = x_1x_2$ (სადაც უხილავი შემადგენლობის კანონი წარმოადგენს კონკატენციას) და ვამუშავებთ ამ ორ შესასვლელს ორ სხვადასხვა ჰეშ ფუნქციასთან ერთად და შემდეგ ვაერთებთ ამ ორ შედეგს $hf(x) = hf_1(x_1)hf_2(x_2)$. სამწუხაროდ ეს პროცედურა არ არის ძალიან ეფექტური. უხეშად რომ ვთქვათ, თითოეული ჰეშ ფუნქცია უერთდება მისი შესასვლელის ბიტებს, მაგრამ არაფერი არ უერთდება ორი შესასვლელის ბიტს ერთად. ამ გაგებით, ყველა შესასვლელი ბიტი უნდა შერეულ იქნას ერთად, რათა უზრუნველყოს რაც შეიძლება დამოუკიდებელი გამოსასვლელი ბიტები. სტინსონმა დაამტკიცა მომდევნო თეორემა. დავუშვათ $HF=\{h_i\}$ არის ϵ-|HB| - თითქმის უნივერსალი ოჯახი HA -დან HB -მდე, და განვსაზღვროთ HF^t როგორც მისი კარტეზიული ნამრავლი $HF^t = \{hf^t_i\}$, სადაც $hf^t_i(x_1,x_2,...x_t) = (hf_i(x_1),hf_i(x_2),...hf_i(x_t))$. მაშინ, HF^t არის ϵ'-|HB|^t - თითქმის უნივერსალი, სადაც $\epsilon' = \epsilon|HB|^{t-1}$. იმ შემთხვევაშიც კი თუ HF უნივერსალურია (ϵ=1), შედეგად მიღებული ოჯახი პირდაპირ სცილდება უნივერსალურობას ($\epsilon' >1$).

მეორე, მოდით განვიხილოთ ჰეშ ფუნქციათა ორი ოჯახი: HF_1, HA_1 -დან HB_1 -მდე, რომელიც არის ϵ_1-|HB_1|- თითქმის უნივერსალი, და HF_2, HA_2 -დან = HB_1 HB_2 -მდე, რომელიც არის ϵ_2-|HB_2|- თითქმის უნივერსალი. მაშინ, შემადგენლობების სიმრავლე $h(x) = hf_2(hf_1(x))$, $HF=\{hf = hf_2 \circ hf_1 : hf_i \in HF_i\}$ არის ϵ-|B2|- თითქმის უნივერსალი, სადაც $\epsilon = \epsilon_1|HB_2|/|B_1| + \epsilon_2$. სამწუხაროდ, იმ შემთხვევაშიც კი როცა ორივე ოჯახი უნივერსალურია ($\epsilon_{1,2} = 1$), შედეგად მიღებული ოჯახი შეიძლება არ იყოს ასე ($\epsilon_1|HB_2|/|HB_1| + \epsilon_2 >1$). მესამე, (39) ფორმულა იმეორებს მცირე ჰეშ ფუნქციას 2hs ბიტებიდან hs ბიტებამდე, რათა

ჩამოაყალიბოს უფრო დიდი ჰეშ ფუნქცია. იგი ეხმარება დიდი შესასვლელი სიდიდეების მიღებაში, მაგრამ შედეგად მიღებული გამოსასვლელი სიდიდე ჯერ კიდევ შემოიფარგლება ძირითადი ჰეშ ფუნქციით. დაბოლოს, გამოსასვლელი სიდიდის გასაზრდელად, შესაძლოა საინტერესო იყოს მცირე გამოსასვლელი სიდიდეების მქონე ჰეშ ფუნქციების გამოყენება შედარებით დიდი გამოსასვლელი სიდიდეების ჩამოსაყალიბებლად. ეს მართლაც რომ შესაძლებელია. დავუშვათ HF_1 არის ჰეშ ფუნქციათა უნივერსალური ოჯახი, რომლის შესასვლელია A და გამოსასვლელი HB_1. დავუშვათ $HF = \{(hf_1,h_2) \mid hf_1,hf_2 \in HF_1\}$ არის ჰეშ ფუნქციათა სიმრავლე, რომლის გამოსასვლელი წარმოადგენს ორ დამოუკიდებლად შერჩეულ ჰეშ ფუნქციათა გამოსასვლელის კონკატენციას. HF -ში კოლიზია ხდება მხოლოდ მაშინ, როცა ორივე შემადგენელი ფუნქცია hf_1 და hf_2 იწვევს კოლიზიას. კოლიზიების რაოდენობა HF -ში შესაბამისად წარმოადგენს თითოეულ შემადგენელ ოჯახში არსებულ კოლიზიების რაოდენობის ნამრავლს,

$$|\{(hf_1(x_1),hf_2(x_1)) = (hf_1(x_2),hf_2(x_2))\}| \le |HF_1|^2/|HB_1|^2 = |HF|/|HB|. \qquad (40)$$

შედეგად მიღებული ოჯახი უნივერსალურია თუ შემადგენელი ოჯახიც უნივერსალურია. ეს ფორმულა შეიძლება განმეორდეს და შესაბამისად გვაძლევს საშუალებას თავისუფლად გავზარდოთ გამოსასვლელი სიდიდე. ამ მეთოდის ნაკლი ის არის, რომ იგი მნიშვნელოვნად ზრდის შეფასების სირთულეს. დავუშვათ $k_1 = \log|HB_1|$ არის HF_1 -ის გამოსასვლელი ბიტების რიცხვი და დავუშვათ, რომ ეს რიცხვი არის ფიქსირებული. გამოსასვლელი $\log|HB|$ ბიტებისთვის, შედგენილმა ჰეშ ფუნქციამ უნდა განახორციელოს $\log|HB|/k_1$, HF_1 -ის ფუნქციათა შეფასებები. ეს რიცხვი პროპორციულია გამოსასვლელი ბიტების რიცხვისა, რომელიც პროპორციულია შესასვლელი ბიტების რიცხვისა. თუ ჩავთვლით, რომ $hf \in HF_1$ -ის შეფასების კომპლექსურობა მინიმუმ პროპორციულია შესასვლელი ბიტების $l = \log|HA|$ რიცხვისა, შედეგად მიღებული ჰეშ ფუნქცია ხდება კვადრატული შესასვლელი / გამოსასვლელი ბიტების რიცხვში. (ჰეშ ფუნქცია

დამოკიდებული უნდა იყოს ყველა შესასვლელ ბიტზე, აქედან გამომდინარე, წრფივი ან მაღალი კომპლექსურობის თეორიაზე). ასეთი ფორმულირება ზოგადია, მაგრამ სამწუხაროდ კომპიუტერულად არაა ეფექტური. ამ ნაწილის დასკვნის სახით, შეგვიძლია ვთქვათ, რომ გამოსასვლელი სიდიდე შესასვლელ სიდიდეზე მეტად უფრო კრიტიკულია. გამოსასვლელი (და შესასვლელი) სიდიდის ხელოვნურად გაზრდის მცდელობა, როგორც პირველ ფორმულაშია, იწვევს ოჯახის უნივერსალურობისგან დაშორებას. ეფექტური ჰეშ ფუნქციები დიდი შესასვლელი სიდიდით არსებობს აუთენტიფიკაციის მოქმედების სფეროში, მაგრამ როგორც წესი მათ აქვთ მცირე გამოსასვლელი სიდიდეები. შეიძლება გავზარდოთ ასეთი ფუნქციების გამოსასვლელი სიდიდე ბოლო ფორმულირების საშუალებით, მაგრამ მაღალი ღირებულება აქვს. ამრიგად, კონფიდენციალურობის გაძლიერების მიზნით, ჩვენ გვჭირდება ჰეშ ფუნქციების ეფექტური ოჯახები, რომლებსაც აქვთ შინაგანად დიდი შესასვლელი და გამოსასვლელი სიდიდეები.

4.3 კონფიდენციალურობის გაძლიერებისთვის შესაფერისი უნივერსალური ოჯახები

ამჯერად ჩვენ ჩამოვთვლით ჰეშ ფუნქციების რამდენიმე უნივერსალურ ოჯახს და განვიხილავთ მათ შესაბამისობას კონფიდენციალურობის გაძლიერებასთან.

4.4 ორობითი მატრიცები

განმარტება 8 დავუშვათ HA = $GF(2)^l$ და HB = $GF(2)^k$. Mes, ha $k \times l$ ორობითი მატრიცისთვის, დავუშვათ $h_M(x) = Mx$ არის M -ის ნამრავლი, სვეტის ვექტორით x. მაშინ, HF3 = $\{hf_{Mes} : Mes \in GF(2)^{k*l}\}$ არის უნივერსალი. ამ ოჯახში ჰეშ ფუნქციის დადგენა, კერძოდ მატრიცა Mes -ის, მოითხოვს kl ბიტებს, რომელიც სამწუხაროდ არ არის მისაღები ჩვენი აპლიკაციისთვის. მაგალითად., $hl \approx 10^5$ -ის შემთხვევაში, იგი საჭიროებს 10^{10} -ის მიმდევრობას გადაცემის განსახორციელებლად. გარდა ამისა, მის შეფასებას აქვს

კვადრატული მნიშვნელობა, $O(khl)$ =ბიტი $O(hl^2)$ ვინაიდან $k=O(hl)$. საბედნიეროდ, შესაძლებელია ზემოთ ხსენებული ოჯახის სიდიდის შეზღუდვა იმის მოთხოვნის საფუძველზე, რომ მატრიცა *Mes* იყოს Toeplitz მატრიცა, ანუ, თუ $Mes_{i,j} = Mes_{i+\delta,j+\delta}$ რომელიმე $i,j,\delta \in \mathbf{N}$ -თვის, ასე რომ $1 \le i,i+\delta \le k$ და $1 \le j,j+\delta \le l$. შედეგად მიღებული ოჯახი $HF3_{,Toeplitz}$ მაინც უნივერსალურია. უპირატესობა ისაა, რომ $k \times l$ Toeplitz მატრიცა მოითხოვს მხოლოდ $k + hl - 1$ ბიტს გადაცემის განსახორციელებლად: იგი მთლიანად განისაზღვრება მისი პირველი რიგისა და პირველი სვეტის მიხედვით.

4.5 მოდულური არითმეტიკა

განმარტება 9 დავუშვათ $HA = \{0,1,\dots \alpha - 1\}$ და $HB = \{0,1,\dots \beta - 1\}$. დავუშვათ hp არის ძირითადი რიცხვი, რასთან ერთადაც $hp \ge \alpha$ და $g_{c,d}(x) = (hcx + hd) \bmod hp$. დავუშვათ $f(x) : \mathbf{Z}_{hp} \to HB$ არის რომელიმე ფუნქცია, ისე რომ $|\{x \in \mathbf{Z}_p : f(x) = y\}| \le \lceil p/\beta \rceil$, $\forall y \in HB$. მაშინ ორივე ფუნქციის შემადგენლობა $hf_{hc,hd}(x) = f(g_{hc,hd}x))$ ქმნის მომდევნო ოჯახს: $H_1 = \{h_{hc,hd} : hc,hd \in \mathbf{Z}_{hp}, c \ne 0\}$. კარტერმა და ვეგმანმა გვიჩვენეს, რომ HF_1 არის უნივერსალური.

ეს ოჯახი ჰეშ ფუნქციის კომპაქტური იდენტიფიკაციის საშუალებას იძლევა. მისი ერთადერთი ნაკლი არის არა-ბინარული ველის გამოყენება. ჩვენი აპლიკაციისთვის უმჯობესია ბიტების დამუშავება. შესაძლებელია თუ არა არითმეტიკული მოდულის გამოყენება ორის ენერგიით? ოჯახი HF_1 პირდაპირ ვერ გამოდგება ძირითადი ხარისხისთვის. ამის ნაცვლად, მოდით შევქმნათ ახალი ოჯახი ამ მიმართულებით.
დავუშვათ α და $\beta, \beta < \alpha$, ორი სრულიად დადებითი მთელი რიცხვი. დავუშვათ $hf_{hc,hd}(x) = \lfloor (hcx+hd \bmod 2^{\alpha})/2^{\alpha-\beta} \rfloor$, β აფინური ფუნქციის ყველაზე მნიშვნელოვანი ბიტები $cx + d$ რომელიც გამოითვლება მთელი რიცხვების მოდულის 2^{α} რგოლში

თეორემა 7. ჰეშ ფუნქციის მომდევნო ოჯახი არის უნივერსალური:

$$HF_{\alpha,\beta} = \{h_{hc,hd} : hc,hd \in \mathbf{Z}_{2^{\alpha}}, \gcd(hc,2) = 1\}. \quad (41)$$

დამტკიცება: შესასვლელის სიდიდე არის $|HA| = 2^{\alpha}$, გამოსასვლელის სიდიდე არის $|HB| = 2^{\beta}$ და ოჯახის სიდიდე არის $|HF\alpha,\beta| = 2^{2\alpha-1}$. იმისათვის რომ დავამტკიცოთ, რომ ეს ოჯახი უნივერსალურია, უნდა ვაჩვენოთ, რომ ფუნქციათა რაოდენობა $HF\alpha,\beta$ -ში, ისე რომ $hf_{hc,hd}(x_1) = hf_{hc,hd}(x_2)$, რომელიმე ფიქსირებული x_1და x_2, $x_1 \neq x_2$ -თვის, შეფასებულია ზედა ზღვრით $|HB\alpha,\beta|/|HB| = 2^{2\alpha-\beta-1}$ მიერ.

დავუშვათ $hf_{hc,hd}(x_1) = hf_{hc,hd}(x_2) = t$, ასე რომ $hcx_1 + hd = 2^{\alpha-\beta}t + u_1$ და $hcx_2 + hd = 2^{\alpha-\beta}t + u_2$, სადაც $u_1,u_2 \in \mathbf{Z}_{2^{\alpha-\beta}}$. ყველა ოპერაცია ხორციელდება მოდული 2^{α} -ით, თუ სხვაგვარად არ არის დადგენილი. პირველი, განვსაზღვროთ t და u_2. გამოკლების საშუალებით hc -მ უნდა დაადასტუროს განტოლება $hc(x_1 - x_2) = u_1 - u_2$. დავუშვათ $\gcd(x_1 - x_2, 2^{\alpha}) = 2^{\delta}$. ვინაიდან u_2 არის ფიქსირებული, $hc(x_1 - x_2)$ ნაპოვნი უნდა იქნას მწკრივში $\{-u_2,\ldots,-u_2+2^{\alpha-\beta}-1\}$. δ -დან გამომდინარე შეიძლება ადგილი ჰქონდეს ორ შემთხვევას: $\delta < \alpha - \beta$ ან $\alpha - \beta \leq \delta < \alpha$. (შემთხვევა $\delta = \alpha$ არ არის შესაძლებელი ვინაიდან $x_1 \neq x_2$). თუ გვაქვს $\delta < \alpha - \beta$, არსებობს 2^{δ} შესაძლო პასუხი hc -სი, როცა კი გვაქვს $2^{\delta} \mid u_1 - u_2$; თუმცა, ვინაიდან hc უნდა იყოს კენტი, გვექნება $2^{\delta+1} ? u_1 - u_2$. თუ $\alpha - \beta \leq \delta < \alpha$, პასუხის ერთადერთი შესაძლო შემთხვევა არის როცა გვაქვს $u_1 = u_2$ ვინაიდან $|u_1 - u_2| < 2^{\alpha-\beta}$; მაგრამ ამ შემთხვევაში არანაირი კენტი პასუხი არ არის შესაძლებელი. ამრიგად, მოდით კონცენტრაცია მოვახდინოთ შემთხვევაზე $\delta < \alpha - \beta$. სიმრავლე $\{-u_2,\ldots,-u_2+2^{\alpha-\beta}-1\}$ შეიცავს $2^{\alpha-\beta-\delta-1}$ სიდიდეებს, ისე რომ სეიძლება ვიპოვოთ 2^{δ} კენტი პასუხები. ამრიგად ფიქსირებული t და u_2 -თვის, არსებობს hc -ს $2^{\alpha-\beta-1}$ სავარაუდო სიდიდე. ნებისმიერი მოცემული hc -თვის, (t,u_2) -ის 2^{α} შესაძლო სიდიდიდან თითოეული განსაზღვრავს ha hd -ის. შედეგად, არ არსებობს $2^{2\alpha-\beta-1}$ -ზე მეტი ჰეშ ფუნქცია $HF\alpha,\beta$ -ში, რომელიც ორი სხვადასხვა შესასვლელისთვის იძლევა იგივე გამოსასვლელს.

მოდით ავღნიშნოთ რამდენიმე ფაქტი ამ ოჯახის ფორმასთან დაკავშირებით. პირველი, მისი ფუნქცია უნდა იყოს აფინური, იმისათვის რომ იყოს უნივერსალური; თუ ავიღებთ წრფივი ფუნქციების (ე.ი. სადაც hd=0) ქვეჯგუფს, შედეგად მიღებული ოჯახი არ იქნება უნივერსალური. იგივე

ითქმის მოთხოვნაზე, რომ c იყოს კენტი; თუ დავუშვებთ, hc -ს ლუწად დაშვება, დაარღვევს უნივერსალურობას. დაბოლოს, ყველაზე ნაკლებად მნიშვნელოვანი (ყველაზე მეტად მნიშვნელოვანი ბიტების ნაცვლად) ბიტების გამოყენება იწვევს არა - უნივერსალურ ოჯახს. ოჯახის წევრის იდენტიფიკაცია მოითხოვს 2hl – 1 ბიტს.

4.6 გამრავლება სასრულ ველებზე

განმარტება 10. დავუშვათ HA = $GF(2^l)$ და HB = $\{0,1\}^k$. დავუშვათ $hf_{hc}(x)$ განისაზღვროს როგორც ნამრავლი hcx -ის პირველი k ბიტები $GF(2^l)$ -ის მრავალწევრიან წარმომადგენლობაში.

სიმრავლე

$$\mathcal{H}_{GF(2^l)\to\{0,1\}^k} = \{hf_{hc}: hc \in GF(2^l)\} \qquad (42)$$

წარმოადგენს ჰეშ ფუნქციათა უნივერსალურ ოჯახს. (გაითვალისწინეთ, რომ k მიღებული ბიტების მდებარეობას მნიშვნელობა არა აქვს იმისათვის, რომ ოჯახი იყოს უნივერსალური).

აღნიშნული ოჯახი არის ბიტზე - ორიენტირებული და მოითხოვს hl ბიტებს, იმისათვის რომ განსაზღვროს კონკრეტული ფუნქცია (ე.ი. c -ს სიდიდე).

გაითვალისწინეთ, რომ ზემოხსენებული ოჯახი არ უნდა ავურიოთ მოცემულ მაგალითში 1. აქ აღებულია მხოლოდ წრფივი ფუნქციები, მაშინ როცა მაგალითი 1 მოითხოვს აფინურ ფუნქციებს. გარდა ამისა, 1 მაგალითში მოცემული ოჯახი ძლიერ უნივერსალურია, ხოლო მე-10 განმარტებაში მოცემული ოჯახი უნივერსალურია მხოლოდ. ამ ოჯახის უფრო დეტალური დახასიათება მოცემულია ქვემოთ.

თავი 5. ჰეშ ფუნქციების იმპლემენტაციის ასპექტები

ამ ნაწილში მოკლედ განვიხილავთ ზემოხსენებული ჰეშ ფუნქციების იმპლემენტაციას და შემდეგ კონცენტრაციას მოვახდენთ ორობით ველში გამრავლებაზე, როგორც ამას მოითხოვს $HF_{GF(2l)\to\{0,1\}k}$.

HF_3 ოჯახი მოითხოვს კვადრატული დროის შეფასებას ვინაიდან ყველა შესაძლო k × 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 ან 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(hlloghlloghlloghl) -ში.

5.1 გამრავლება ორობით ველში

ჩვენ ახლა განვიხილავთ $HF_{GF(2^l)\to\{0,1\}^k}$ ოჯახის იმპლემენტაციას, რომელიც დაფუძნებულია ორობით ველში გამრავლებაზე, რაც განსაზღვრულია მე-10 განმარტებაში. 7.2 ნაწილში წარმოდგენილი ოჯახებიდან, ეს ოჯახი შეირჩა მისი ბიტების ყველაზე მცირე რაოდენობის გამო, რომელიც საჭიროა ოჯახში წევრის იდენტიფიკაციისთვის. აგრეთვე, იგი გამოყენებულ იქნა QKD-ის ექსპერიმენტული განხორციელებისთვის თანმიმდევრული მდგომარეობებით. კერძოდ, შეგვიძლია აღვწეროთ ამ კონკრეტული ოპერაციის განხორციელების სავარაუდო გზა დიდი ბლოკების ეფექტურად დამუშავების მიზნით. $GF(2^l)$ -ის ორი ელემენტის გამრავლება შეიძლება

შესრულდეს კვადრატულ დროში ტრადიციული shift-and-add ალგორითმის გამოყენებით. თუმცა, ეს საკმაოდ შეანელებს ოპერაციას, განსაკუთრებით მაშინ თუ მოგვიწევს ბლოკური სიდიდის გაზრდა. ნაცვლად ამისა, ჩვენ ავღწერთ მარტივ ალგორითმს, რომელიც ასრულებს გამრავლებას cllogl ოპერაციებში მთელ რიცხვებზე ზოგიერთი მცირე კონსტანტასთვის hc. სინამდვილეში ეს ნიშნავს, რომ cllogl ოპერაციები დამაკმაყოფილებელია იმ პირობით თუ logl სიდიდის რიცხვები შესული იქნება მექანიზმის რეგისტრში. 64 - ბიტიანი პროცესორების სტანდარტულად გახდომის შემთხვევაში, მაინც გვექნება კომფორტული ზღვარი. თეორიაში, ასიმპტომური კომპლექსურობა არის OK(hlloghlloghlloghl) -ში.

იმპლემენტაცია ეყრდნობა რიცხობრივ-თეორიულ გარდაქმნას. $GF(2^l)$ გამრავლებიდან NTT-მდე დაყვანა მიმდინარეობს შემდეგნაირად:

- პირველი, $GF(2^l)$ გამრავლება იკვეცება ორობით მრავალწევრიან $\mathbf{Z}_2[x]$ რგოლში გამრავლებაზე, რომელიც მოიცავს მოდული hp(x) -ის შეკვეცას, სადაც p(x) არის ხარისხი hl -ის უკვეცი მრავალწევრიანი $\mathbf{Z}_2[x]$ -ში.
- მეორე, $\mathbf{Z}_2[x]$ -ში გამრავლება იკვეცება $\mathbf{Z}[x]$ -ში გამრავლებამდე, ანუ მთელ რიცხვიანი კოეფიციენტების მქონე მრავალწევრიანების რგოლი, რომელიც მოიცავს მისი კოეფიციენტების mod 2 შეკვეცას.
- მესამე, $\mathbf{Z}[x]$ გამრავლება იკვეცება $\mathbf{Z}_m[x]/(x^L-1)$ გამრავლებად, მრავალწევრიანების რგოლი, რომელიც მოიცავს კოეფიციენტებს $\mathbf{Z}_m$ და modulo x^L-1 -ში (ე.ი. x -ის ხარისხით მიღებულ უნდა იქნას modL, $x^L = x^0 = 1$). ეს იმ პირობით ამართლებს, თუ მრავალწევრიანები შეზღუდული არიან გამრავლებისთვის საკუთარი ხარისხით და კოეფიციენტების სიდიდით. ეს არ წარმოადგენს პრობლემას, ვინაიდან გასამრავლებელი მრავალწევრიანები მომდინარეობენ $GF(2^l)$ - დან. ადვილად შეიძლება იმის შემოწმება, რომ იგი ამართლებს იმ შემთხვევაში თუ mes >2hl და L >2l.
- დაბოლოს, გამრავლება $\mathbf{Z}_m[x]/(x^L - 1)$ -ში შეიძლება განხორციელდეს პირველ რიგში ორივე ოპერანდის კოეფიციენტის გარდაქმნით NTT გამოყენებით, კომპონენტურად გამრავლებით და შემდეგ, შედეგად მიღებული

კოეფიციენტების გარდაქმნით შებრუნებული NTT -ის გამოყენებით - იხილეთ ნაწილი 7.3.2.

პირველი შეკვეცის განსახორციელებლად, საჭიროა გვქონდეს hl ხარისხის უკვეცი მრავალწევრიანი. ჩვენ დაინტერესებული ვართ დიდი ბლოკური სიდიდეებით, და მაღალი ხარისხის უკვეცი მრავალწევრიანები ადვილი საპოვნელი არაა. ბრენტი, ლარვალა და ზიმერმანი გვიჩვენებენ, თუ როგორ შევამოწმოთ სამწევრიანების (ე.ი. $x^l + x^{hs} + 1$ ფორმის მრავალწევრიანები) კვეცადობა GF(2) -ზე ეფექტურად. ისინი ასევე გვთავაზობენ l ხარისხის ბევრი უკვეცი მრავალწევრის ჩამონათვალს, სადაც l მერსენის ხარისხის მაჩვენებელია, ანუ, ისე რომ $2^{hl} - 1$ არის მარტივი რიცხვი. მათი იმპლემენტაციის ჩანაწერთა ფაილების ნახვა შესაძლებელია და ამ ეტაპზე ისინი გვთავაზობენ 127, 521, 607, 1279, 2281, 3217, 4423, 9689, 19 937, 23 209, 44 497, 110 503, 132 049, 756 839, 859 433, 3 021 377 და 6 972 593 ხარისხების უკვეცად მრავალწევრებს.

შერჩეული ველი არის $GF(2^{110\,503})$. 110 503 ხარისხის მქონე ველის შერჩევის მიზეზი მერსენის შესაძლო ხარისხის მაჩვენებლებიდან მდგომარეობს იმაში, რომ NTT ყველაზე ეფექტურად ხორციელდება მაშინ როდესაც L არის ორის ხარისხი, $L = 2^{\lambda}$. ვინაიდან უნდა გვქონდეს $L > 2l$, მოცემული $110\,503 < 131\,072 = 2^{17}$ უფრო ახლოს იყო მომდევნო ორის ხარისხთან ვიდრე ეს $132\,049 < 262\,144 = 2^{18}$. ამ ველის წარმოსადგენად, სავარაუდო უკვეცი სამწევრები არიან $x^{110\,503} + x^{25\,230} + 1$, $x^{110\,503} + x^{53\,719} + 1$, $x^{110\,503} + x^{56\,784} + 1$ და $x^{110\,503} + x^{85\,273} + 1$, სადაც ბოლო ორი მრავალწევრი პირველი ორის შექცეული სიდიდეებია.

5.2 რიცხობრივ - თეორიული გარდაქმნა

ამჯერად დეტალურად განვიხილოთ გამრავლება NTT -ის გამოყენებით. მოცემულია $\mathbf{Z}_m[x]/(x^L - 1)$ -ის ორი ელემენტი, ვთქვათ $r(x) = \sum_{i=0}^{L-1} r_i x^i$ და $s(x) = \sum_{i=0}^{L-1} s_i x^i$, მათი ნამრავლი ამ რგოლში არის $isr(x)s(x) = t(x) = \sum_{i=0}^{L-1} t_i x^i \quad t_i = \sum_{j=0}^{L-1} r_{i-j} s_j$, -თან ერთად, სადაც სუბსკრიპტები უნდა აღვიქვათ L მოდულად.

განმარტება 11. $\mathbf{Z}_{mes}$,-ში დავუშვათ ω არის L-th ერთეულის ფესვი, ანუ, $\omega^L = 1$ და $\omega^{L'} \neq 1$, $0 < L' < L$ -თვის. მოცემულია ვექტორი $\mathbf{r} = (r_i)_{i=0\ldots L-1}$, $r_i \in \mathbf{Z}_m$ -ით, განვსაზღვროთ $\mathbf{r}$ **-ის** NTT როგორიცაა $\mathcal{F}\mathbf{r} = \mathbf{R} = \left(R_j\right)_{j=0\ldots L-1,}$ $R_j = \sum_{i=0}^{L-1} r_i \omega^{ij}$ -თან ერთად.

ამის შემდეგ, ვივარაუდოთ, რომ mes= hp არის მარტივი რიცხვი. მიუხედავად იმისა, რომ NTT დასაშვებია შედგენილი mes -თვის, ისინი ნაკლებად ეფექტურია. ვინაიდან ρ-th ერთეულის ფესვები მხოლოდ ხელმისაწვდომია მაშინ, როცა ρ იყოფა hp–1, უნდა გვქონდეს hp =vL+1 ზოგიერთი მთელი რიცხვისთვის v. NTT -ის (იხილეთ ქვემოთ) ეფექტური განხორციელებისთვის, უნდა გვქონდეს $L = 2^{\lambda}$ და შესაბამისად $hp=v2^{\lambda}+1$. NTT შეიძლება შესრულდეს $c_{NTT}LlogL$ მთელი რიცხვის ოპერაციებში თუ L წარმოადგენს ორის ხარისხს, ზოგიერთი კონსტანტასთვის c_{NTT}. პრინციპი ზუსტად იგივეა სწრაფი ფურიეს გარდაქმნის შემთხვევაში (FFT); უბრალოდ საჭიროა Lth ერთეულის ფესვის ჩანაცვლება კომპლექსურ რიცხვებში $\omega = e^{i2\pi/L}$, $\mathbf{Z}_p$ -ში არსებული Lth ერთეულის ფესვით, რომელიც განსაზღვრულია ზემოთ. დანარჩენისთვის, იგი შეუცვლელად მოქმედებს და FFT შეიძლება მაინც დაეყრდნოს "პეპელისებრ" ოპერაციას, როგორიცაა $\omega^{L/2} = -1$ ორივე შემთხვევაში. NTT -ის გამოყენების უპირატესობა მდგომარეობს იმაში, რომ კონვოლუციების განხორციელება შესაძლებელია ეფექტურად. დავუშვათ ანაბეჭდი ვექტორები შეიცავენ შესაბამისი რომანული მრავალწევრების კოეფიციენტებს. t(x)=r(x)s(x) -ის გამოთვლა ექვივალენტურია კონვოლუციის გამოთვლისა $\mathbf{t} = \mathbf{r} * \mathbf{s}$, სადაც $t_j = \sum_{i=0}^{L-1} r_{j-i}s_i$. NTT -ის გამოყენებისას, $F(\mathbf{r} * \mathbf{s}) = (\mathcal{F}\mathbf{r}) \cdot (\mathcal{F}\mathbf{s})$, სადაც· აღნიშნავს კომპონენტურ ნამრავლს t,$T_j = R_jS_j$.

იმისათვის, რომ ვიპოვოთ **t, T** = F(**t**) -დან, გამოყენებულ უნდა იქნას შექცეული NTT. იგი მოქმედებს პირდაპირის მსგვასად, მაგრამ ნაცვლად ამისა, ω^{-1} ერთეულის Lth ფესვის შექცევით: $t_i = \sum_{j=0}^{L-1} T_i\omega^{-ij}$.

მაგალითად, დავუშვათ $L = 2^{18} = 262\,144$. $L + 1 = 262\,145 = 5 \times 52\,429$ და $2L + 1 = 524\,289 = 3 \times 174\,763$ შედგენილია, მაშინ როცა $3L + 1 = 786\,433$ = p არის

მარტივი რიცხვი, ამრიგად $v = 3$. $\mathbf{Z}_{786\,433}$ -ში უმცირესი გენერატორი არის $g = 11$, ანუ $g^{p-1} = 1$, მაშინ როცა არც ერთი ხარისხის მაჩვენებელი არ იღებს ამ ხარისხს. მაშინ, ამ $\omega = g^v = 11^3 = 1331$ ასპექტით, ვიღებთ ($\omega^{262\,144} = 1$) ერთეულის 262 144 ფესვს. გაითვალისწინეთ, რომ როგორც ნავარაუდებია, $\omega^{131\,072} = -1$, რომელიც იძლევა „პეპელისებრი“ ოპერაციის შესაძლებლობას. დაბოლოს, ჩვენ უნდა გამოვთვალოთ $\omega^{-1} = 104\,582$ შექცეული NTT -თვის.

5.3 რიცხობრივი - თეორიულ გარდაქმნებზე დაფუძნებული ოჯახი

რადგან NTT მძლავრი საშუალება ჩანს, მოდით გვერდით გადავდოთ გამრავლება სასრულ ველში და ვნახოთ შეგვიძლია თუ არა შევქმნათ NTT -ზე დაფუძნებული ჰეშ ფუნქციის უნივერსალური ოჯახი.

$\mathcal{H}_{\mathrm{GF}(2^l)\to\{0,1\}^k}$ ფუნქციის შესაფასებლად, NTT უზრუნველყოფს სწრაფ გამრავლებას $\mathbf{Z}_p[x]/(x^L - 1)$ -ის რგოლში. უშუალოდ ამ რგოლში მუშაობით, ჩვენ თავს ავარიდებთ 7.3.1 ნაწილში აღწერილ შეკვეცებს და უფრო პირდაპირ მივუდგებით NTT -ს საუკეთესო იმპლემენტაციის შესრულებისთვის. უფრო კონკრეტულად, რომ ვთქვათ, შეგვიძლია დავამუშაოთ დაახლოებით $L\log p$ შესასვლელი ბიტი ერთ ჯერზე ნაცვლად მხოლოდ $l < L/2$-ისა.

ჩვენ რეალურად განვიხილავთ ჰეშ ფუნქციების ორ ექვივალენტურ ოჯახს. ეს ორი ოჯახი ექვივალენტურია უნივერსალურობის თვალსაზრისით. ერთს აქვს ისეთი ფორმა, რომელიც აადვილებს მის იმპლემენტაციას, ხოლო მეორეს აქვს მოსახერხებელი ალგებრული ინტერპრეტაცია.

განმარტება 12. დავუშვათ $1 \le \beta \le L$. $\mathbf{C}, \mathbf{R} \in \mathbf{Z}_p^L$ -თვის და ისე რომ $\mathbf{C}$ არ აქვს არა ნულოვანი ელემენტი, $C_i \neq 0 \forall i = 0 \dots L-1$, დავუშვათ $h_{\mathbf{C}}(\mathbf{R}) = (\mathcal{F}^{-1}(\mathbf{C} \cdot \mathbf{R}))_{0\dots\beta-1}$ არის შექცეული NTT მათი კომპონენტური ნამრავლისა, ვიღებთ მხოლოდ შედეგის β პირველ ელემენტებს. მოდით განვსაზღვროთ ოჯახი $\mathcal{H}_{p,L,\beta} = \{h_{\mathbf{C}} : C_i \neq 0 \forall i\}$.

განმარტება 13. დავუშვათ $1 \le \beta \le L$. $c,r \in \mathbf{Z}_p[x]/(x^L-1)$-თვის და ისე რომ c ჰქონდეს მულტიპლიკატური შექცევადობა, დავუშვათ $h'_c(r) = crmod\, x^\beta$ არის მათი ნამრავლი, β და უფრო მაღალი ხარისხის x -ის უგულებელყოფის შემთხვევაში. მოდით განვსაზღვროთ ოჯახი

$$\mathcal{H}'_{p,L,\beta} = \{h_c : \&c^{-1}\exists\} \qquad (43)$$

შეიძლება თუ არა მულტიპლიკატური შექცევადობა $\mathbf{Z}_p[x]/(x^L - 1)$ -ში მარტივად განისაზღვროს მისი NTT -დან: ელემენტი c აქვს შექცევადობა თუ მისი კოეფიციენტების NTT $\mathbf{C} = F(\mathbf{c})$ არა აქვს ნული $C_i \neq 0\ \forall i = 0...L-1$. ეს გამომდინარეობს $\mathbf{Z}_p$ -ის ხარისხიდან, რა შემთხვევაშიც NTT კოეფიციენტების ყოველი გამრავლება შეიძლება შებრუნდეს თუ სამრავლი არა - ნულოვანია. გამომდინარე $t = cr$ -დან, ჩვენ გვაქვს $\mathbf{t} = F^{-1}(F(\mathbf{c})\cdot F(\mathbf{r})) = F^{-1}(\mathbf{C}\cdot\mathbf{R})$, სადაც $\mathbf{C} = F(\mathbf{c})$ and $\mathbf{R} = F(\mathbf{r})$. ასე რომ, ჰეშ ფუნქციის აღწერა $\mathcal{H}'_{p,L,\beta}$ -ში $\mathbf{c}$ ან $\mathbf{C}$ -თი აშკარად ერთიდაიგივეა. იგივე არგუმენტი ვრცელდება შესასვლელ $\mathbf{r}$ -ზე. სხვა სიტყვებით, რომ ვთქვათ ეს ორი ოჯახი შესასვლელების გადანაცვლების ექვივალენტურია, შესაბამისად ისინი იზიარებენ უნივერსალურობის ერთიდაიგივე თვისებებს: $\mathcal{H}'_{p,L,\beta}$ არის $\epsilon/|HB|$- თითქმის უნივერსალი თუ $\mathcal{H}'_{p,L,\beta}$ არის $\epsilon/|HB|$- თითქმის უნივერსალი $|HB| = p^\beta$ გამოსასვლელი სიდიდით.

თეორემა 8. თუ $p - 1 \ge L$, ორივე $\mathcal{H}_{hp,L,\beta}$ და $\mathcal{H}'_{hp,L,\beta}$არის $\frac{hp^\beta}{(hp-1)^\beta}/|H\mathcal{B}|$- თითქმის უნივერსალი.

დამტკიცება: ჩვენ ამას ვამტკიცებთ მხოლოდ $\mathcal{H}_{hp,L,\beta}$ შედეგისთვის, რომელიც ასევე უშუალოდ ვრცელდება $\mathcal{H}'_{hp,L,\beta}$ -ზე.

შესასვლელის სიდიდე არის $|HA| = hp^L$, გამოსასვლელის არის $|HB| = hp^\beta$ და ოჯახის სიდიდე არის $|\mathcal{H}_{p,L,\beta}| = (hp-1)^L$. ამ თეორემის დასამტკიცებლად, ნაჩვენები უნდა იქნას, რომ ფუნქციების რაოდენობა $\mathcal{H}_{hp,L,\beta}$ -ში, ისე რომ $hf_hc(\mathbf{R}^{(1)}) = hf_hc(\mathbf{R}^{(2)})$, ნებისმიერი ფიქსირებული $\mathbf{R}^{(1)}$ და $\mathbf{R}^{(2)}$, $\mathbf{R}^{(1)} \neq \mathbf{R}^{(2)}$ -თვის, ზედა ზღვარი ფასდება $(hp-1)^{L-\beta}$ -ით.

მოცემული $\mathbf{R}$ -თვის, ჰეშ ფუნქციების შედეგი შედგება β სიდიდეებისგან $t_i = \sum_{i=0}^{L-1} \omega^{-ij} hC_j R_j, i = 0 \dots \beta - 1$. დავუშვათ $\Delta\mathbf{R} = \mathbf{R}^{(1)} - \mathbf{R}^{(2}$. იმისათვის რომ β სიდიდეები იყოს თანაბარი, უნდა გვქონდეს

$$\sum_{j=0\dots L-1} \omega^{-ij} C_j \Delta R_j = 0, i = 0 \dots \beta - 1 \quad (7.1)$$

მოდით პირველ რიგში განვიხილოთ სისტემა (7.1) განტოლებაში, სადაც ΔR_j უცნობებია. სისტემის მატრიცა არის $\beta \times L$ მატრიცა $Mes=(\omega^{-ij}C_j)_{i,j}$. ვანდერმონდეს მატრიცის ხარისხებიდან და $hC_j \neq 0$ ფაქტიდან გამომდინარე, Mes არის β -ის მწკრივი. მოთხოვნა, რომ $p-1 \geq L$ უზრუნველყოფს იმას, რომ მატრიცას არ ჰქონდეს პროპორციული სვეტები. იმისათვის რომ გადავჭრათ ერთგვაროვანი სისტემა (7.1) განტოლებაში, უნდა გვქონდეს სულ მცირე β სხვადასხვა პოზიცია რა შემთხვევაშიც $\Delta Rj \neq 0$.

მოდით განვიხილოთ სისტემა (7.1) განტოლებაში, სადაც C_j უცნობებია. სისტემის მატრიცა არის $\beta \times L$ მატრიცა $Mes' = (\omega^{-ij}\Delta R_j)_{i,j}$. კვლავ, ვანდერმონდეს მატრიცის ხარისხებიდან და იმ ფაქტიდან გამომდინარე, რომ ΔR_j არა - ნულოვანია სულ მცირე β პოზიციებისთვის, Mes′ არის ასევე β -ის მწკრივის. ამგვარად, სისტემა $Mes'\mathbf{C} = 0$ აქვს β განზომილების ვექტორული სივრცე, პასუხის სახით. ამ პასუხებიდან $(hp - 1)^{L-\beta}$ აქვს არა - ნულოვანი კომპონენტები.

ასეთი ჰეშ ფუნქციები შეიძლება განხორციელდეს ძალიან ეფექტურად. უბრალოდ უნდა გავამრავლოთ შესასვლელის თითოეული კომპონენტი შემთხვევითად შერჩეულ მთელ რიცხვთან 1 და hp–1-შორის, შემდეგ გამოყენებულ იქნას NTT შედეგზე და ბოლოს აღებულ იქნას ნიმუშების სასურველი რაოდენობა. მოდით შევადაროთ გამრავლებას ორობით ველზე, რომელიც განხორციელდა 7.3 ნაწილში.

დავუშვათ NTT შესასრულებლად საჭირო არითმეტიკული ოპერაციების რიცხვი არის $c_{NTT}LlogL$. $HF_{GF(2l)\to\{0,1\}^k}$, ფუნქციისთვის, ჩვენ გვაქვს $L \approx 2hl$, ამრიგად NTT გამოსათვლელად საჭირო ეტაპების რაოდენობა ასეთი ჰეშ ფუნქციის შესაფასებლად არის $2c_{NTT}hllogh l$, ამას დამატებული ზოგიერთი წევრი, რომელიც hl -ის პროპორციულია. აქ ჩვენ ვაიგნორებთ ყველა ხარისხს,

რომელიც საჭიროებს შეკვეცას $GF(2^l)$ დან $\mathbf{Z}_m[x]/(x^L - 1)$ -მდე, რადგან ყველა მათგანი l -ის პროპორციულია. შესასვლელი ბიტების რიცხვი არის hl , ასე რომ ეს გვაძლევს $2c_{NTT}$ loghl არითმეტიკულ ოპერაციებს თითოეულ გადამუშავებულ ბიტზე.

NTT, რომელიც გამოიყენება HFhp,L,β ფუნქციის შესაფასებლად, ასევე იღებს c_{NTT}LlogL. აქ, ჩვენ გვაქვს L ≈ hp და NTT იღებს დაახლოებით c_{NTT}LlogL ≈ c_{NTT}L loghp ხარისხებს. მიუხედავად ამისა, აქ NTT ამუშავებს დაახლოებით Lloghp ბიტების შესასვლელ სიდიდეს, შესაბამისად იძლევა c_{NTT} ოპერაციებს თითოეულ გადამუშავებულ ბიტზე. მაგალითად, hl ≈ 2^{17} -ის შემთხვევაში, HFhp,L,β -ში ფუნქციის შეფასება იქნება 34 -ჯერ უფრო სწრაფი ვიდრე $HF_{GF(2l)\to\{0,1\}k}$ -ის შემთხვევაში, რომლის იმპლემენტაციაც აღწერილია ზემოთ.

ამ მნიშვნელოვანი პრაქტიკული დაჩქარების გარდა, ეს ოჯახი განიცდის ორ უმნიშვნელო ნაკლოვანებას. პირველი ის არის, რომ ოჯახი არ არის უნივერსალური - მხოლოდ ახლოსაა უნივერსალურობასთან. მიუხედავად ამისა, უნივერსალურობასთან დაკავშირებით განსხვავება შეიძლება ძალიან მცირე იყოს თუ შერჩეული მარტივი რიცხვი hp საკმარისად დიდია. მეორე ნაკლი არის ის, რომ შესასვლელი და გამოსასვლელი არ არის ორობითი. შესასვლელის შემთხვევისთვის, ეს არ არის პრობლემა, ვინაიდან უნივერსალურობა შეუძლებელია შემცირდეს თუ ჩვენ დავიყვანთ შესასვლელ სიდიდეს ორის ხარისხზე. ამრიგად, შეგვეძლება მაშინვე გამოვიყენოთ ორობითი შესასვლელი სიდიდე. გამოსასვლელის შემთხვევისთვის, შეიძლება არ იყოს კარგი იდეა $\mathbf{Z}_{hp}$ -ის თითოეული ელემენტის გარდაქმნა ⌈loghp⌉ ბიტებად, ვინაიდან შედეგი არ იქნება ერთგვარი. მიუხედავად ამისა, თუ ვინმე მიიღებს ცვლადი - სიდიდის გამოსასვლელს, უარყოფა შეიძლება იყოს ერთგვარი ბიტების მიღების გზა: ვინაიდან hp აქვს hp = ν 2^{λ} + 1 -ის ფორმა, უარყოფა ხდება მხოლოდ მაშინ როცა t_i = hp – 1.

ამ თავში ჩვენ ვიხილეთ ჰეშ ფუნქციების სხვადასხვა სახის ოჯახები და როგორ ვრცელდება ისინი კონფიდენციალურობის გაძლიერების მიზნებზე.

განვმარტეთ რატომ არის საჭირო დიდი შესასვლელი და გამოსასვლელი სიდიდეები და რატომ არის მნიშვნელოვანი გავხადოთ ასეთი ჰეშ ფუნქციების შეფასება ეფექტური. დაბოლოს, განვიხილეთ ჰეშ ფუნქციების უნივერსალური ოჯახების იმპლემენტაციის ასპექტები. იმისათვის რომ კონფიდენციალურობის გაძლიერება სწორად ამოქმედდეს, ელისს და ბობს უნდა ჰქონდეთ თანაბარი შესასვლელები. მათი კორელაციური ზომისა და მოდულაციის მწკრივების X და Y -ის გარდასაქმენლად თანაბარ მწკრივებად Ψ, უნდა შესწორდეს შეცდომები.

თავი 6. რეკონსილიაცია (შეთანხმება)

შეთანხმება არის მეთოდი, რომელიც საჭიროა იმის უზრუნველსაყოფად, რომ კლოდის და დომინიკის გასაღების ელემენტები იყოს თანაბარი. X და Y შემთხვევითი ცვლადების შედეგებიდან გამომდინარე, ისინი უნდა შეთანხმდნენ თანაბარ მწკრივზე Ψ.

ამ თავში, პირველ რიგში წარმოგიდგენთ ზოგად თვისებებს და შემდეგ მიმოვიხილავთ და გაგაცნობთ შეთანხმების მეთოდების რამდენიმე კლასს.

6.1 ამოცანის აღწერა

ლეგიტიმური მხარეების მიზანია მოახდინონ საიდუმლო გასაღების დისტილაცია, ე.ი. შეწყვიტონ საერთო ოროზითი მწკრივი, რომელიც უცნობია ევასთვის. შეთანხმებად მივიჩნევთ, რომ კლოდის X -ის შედეგები განსაზღვრავს საერთო გასაღებს K. კონფიდენციალურობის გამყარებამდე, საერთო მწკრივი Ψ შეიძლება გამოიხატოს Ψ(X) ფუნქციის სახით.

შეთანხმება მოიცავს შეტყობინებების გაცვლას საჯარო კლასიკური აუთენტიფიცირებული არხით, რომელიც ერთობლივად აღინიშნება Mes -ით, ისე რომ დომინიკს შეუძლია Ψ -ის აღდგენა Mes -დან და Y -ის შედეგებიდან. თუ ავღნიშნავთ, როგორც $x_{hl...l}$ ha, X დამოუკიდებელი შედეგების hl ვექტორს, $\Psi(x_{1...l})$, $(\Psi(x_1),...,\Psi(x_l))$ მწკრივი შეიძლება შეიკუმშოს, რათა მივიღოთ დაახლოებით hlHF(Ψ(X)) საერთო ერთგვარი ბიტები.

როგორც მე-6 თავშია განმარტებული, რეკონსილიაციის გავლენა კონფიდენციალურობის გაძლიერებაზე გულისხმობს |Mes| ბიტების შემცირებას გასაღების სიგრძეში, სადაც |Mes| არის რეკონსილიაციის პროცესში გაცვლილი ბიტების რაოდენობა.

ამრიგად, ჩვენი მიზანია HlHF(Ψ(X))–|Mes| -ის მაქსიმალურად გაზრდა, ან Ψ -ის შემთხვევაში, გამოვლენილი ბიტების |Mes| რიცხვის შემცირება.

6.2 რეკონსილიაციის (შეთანხმების) პროტოკოლების მახასიათებლები

სანამ გადავალთ რეკონისილიციის დეტალებზე, მოდით განვიხილოთ ზოგიერთი მისი მახასიათებელი.

პირველი, რეკონსილიაცია შეიძლება იყოს ცალმხრივი ან ინტერაქტიული. პირველი შემთხვევა აშკარად შესაძლებელია მხოლოდ ცალმხრივი საიდუმლო გასაღების დისტილაციისას, რადგან ინფორმაცია იგზავნება მხოლოდ კლოდიდან დომინიკის მისამართით. მეორე შემთხვევაში, კლოდი და დომინიკი ცვლიან ინფორმაციას ორივე გზით.

შესაბამისად, შესათანხმებელი X და Y შემთხვევითი ცვლადები შეიძლება იყოს დისკრეტული ან უწყვეტი. ორივე შემთხვევაში, საერთო მწკრივის Ψ მისაღებად საჭიროა იყოს დისკრეტული, რომელიც დეტალურადაა აღწერილი ნაწილი 6.6 -ში. უწყვეტი ცვლადების შემთხვევა განხილულია მე -9 თავში.

დისკრეტული შემთხვევითი ცვლადების X და Y შემთხვევაში, ისინი შეიძლება იყოს ორობითი, როცა X=Y= {0,1} ან სხვა შემთხვევაში, არა-ორობითი. განვასხვავებთ ორობით (ბინარული) და არა-ორობით (არა-ბინარული) შეთანხმებას, რადგან ორობითი შეთანხმება უფრო ხშირად შეისწავლება ვიდრე არა -ორობითი. ორობითი შეთანხმების პროტოკოლების მაგალითების ნახვა შესაძლებელია 8.3 -დან 8.5 -მდე ნაწილებში. დაბოლოს, შეთანხმების პროტოკოლი შეიძლება ორიენტირებული იყოს ცალკეული სიმბოლოების ან ბლოკების დაშიფვრაზე. ეს განსხვავება არ არის მნიშვნელოვანი, რადგან ბლოკები შეიძლება მიჩნეულ იქნას დიდი მოცულობის ცალკეულ სიმბოლოებად. მიუხედავად ამისა, ამ ვარიანტების გათვალისწინება შეიძლება დაგვეხმაროს შემდგომ დისკუსიაში.

6.3 შეთანხმების ძირითადი ზღვრები

კლოდს და დომინიკს ერთი და იგივე მწკრივის მიღება სურთ და ჩვენ კვლავ მივიჩნევთ, რომ სამიზნე არის კლოდის გასაღების ელემენტები, ან მისი ფუნქცია Ψ(X). ოპტიმიზაციის კრიტერიუმი წარმოადგენს გამოვლენილი ბიტების რაოდენობას, რომელიც საჭიროა ერთი და იგივე მწკრივის მისაღებად. ინტერაქტიული შეთანხმება უფრო უკეთესია თუ ცალმხრივი შეთანხმება? პრინციპში, მხოლოდ დომინიკს სჭირდება კლოდისგან ინფორმაციის მიღება, მაგრამ ინტერაქტიულობა ხელს უწყობს შეცდომების სწრაფად დავიწროვებაში შესწორების მიზნით.

ცალმხრივი შეთანხმებისთვის, პროტოკოლი მარტივი ასაღწერია. კლოდმა დომინიკის უნდა გაუგზავნოს X ფუნქცია, კერძოდ α(X), ისე რომ მან შეძლოს

X -ის აღდგენა Y -ის ცოდნით. ეს პროცესს, რომელსაც უწოდებენ საწყის კოდირებას მეორეხარისხოვანი მონაცემებით.

საწყისი კოდირება მეორეხარისხოვანი მონაცემებით წარმოადგენს უფრო ზოგადი ცნების განსაკუთრებულ შემთხვევას, რომელსაც უწოდებენ განაწილებულ საწყის კოდირებას, სადაც ორი ურთიერთდაკავშირებული წყარო შეკუმშულია დამოუკიდებლად. გასაკვირია, რო სლეპიანმა და ვულფმა გვიჩვენეს, რომ პრინციპში ორივე წყარო შეიძლება შეიკუმშოს იგივე ტემპით როგორც ეს იქნებოდა მათი ერთად ყოფნის შემთხვევაში. ეს ჩამოყალიბებულია მე -9 თეორემაში.

თეორემა 9. დავუშვათ X და Y არის შემთხვევითი ცვლადები, სავარაუდოდ ურთიერთდაკავშირებული. დავუშვათ იქ არის ორი დამოუკიდებელი შიფრატორი, ერთი R_X კოეფიციენტით, რათა დაშიფროს X და მეორე R_Y კოეფიციენტით, რათა დაშიფროს Y. დეშიფრატორისთვის მისაღწევი კოეფიციენტის მდებარეობა, იმისათვის რომ შეძლოს ორივეს X და Y -ის გაშიფვრა მოცემულია შემდეგი ფორმულით:

$$R_X \geq HF(X|Y), R_Y \geq HF(Y|X), R_X + R_Y \geq HF(X,Y). \quad (44)$$

მეორეხარისხოვანი მონაცემებით საწყისი კოდირების ამოცანა არის განაწილებული საწყისი კოდირების განსაკუთრებული შემთხვევა, სადაც ერთ ერთი წყარო იკუმშება შექცევადი გზით. ამის შესახებ დეტალურად მოცემულია 1 დასკვნაში.

დასკვნა 1. დავუშვათ X და Y არის როგორც მე-9 თეორემაშია. ჩავთვალოთ, რომ R_X არის კოეფიციენტი X -ის დასაშიფრად (Y -ის ცოდნის გარეშე). ჩავთვალოთ, რომ Y გადაეცემა დეშიფრატორს. დეშიფრატორისთვის მისაღწევი კოეფიციენტის მდებარეობა, იმისათვის რომ შეძლოს X -ის გაშიფვრა Y -ის ცოდნით, მოცემულია შემდეგი ფორმულით:

$R_X \geq HF(X|Y)$.

ცალმხრივი შეთანხმების პერსპექტივაში, სლეპიანის და ვულფის შედეგი გულისხმობს, რომ კლოდმა უნდა გაგზავნოს სულ მცირე $HF(\Psi(X)|Y)$ ინფორმაციის ბიტები. შესაბამისად, უნდა ჩავთვალოთ, რომ მსმენელი იძენს

იგივე რაოდენობის ინფორმაციის ბიტს $\Psi(X)$ -ზე. შეგვიძლია აღნიშნულის გაკეთება უფრო უკეთესად ინტერაქტიული შეთანხმებით? პრინციპში, გიჩვენებთ, რომ ინტერაქტიული შეთანხმების პროტოკოლმა ასევე უნდა გამოავლინოს სულ მცირე $HF(\Psi(X)|Y)$ ბიტი $\Psi(X)$ -ზე.

თეორემა 10. შეთანხმების პროტოკოლი ამჟღავნებს სულ მცირე $HF(\Psi(X)|Y)$ ბიტს $\Psi(X)$ -თან დაკავშირებით ორივეს, ცალმხრივი და ინტერაქტიული შემთხვევებისას.

დამტკიცება

სიმარტივისთვის, განვიხილოთ სამ - ხარისხიანი ინტერაქტიული პროტოკოლის შემთხვევა - ადვილია მისი გენერალიზება უფრო მაღალი რიცხვის ხარისხებად. კლოდი უგზავნის Mes_1 შეტყობინებას დომინიკს, რომელიც პასუხობს კლოდს Mes_2 შეტყობინებით, რომელიც თავის მხრივ, უგზავნის Mes_3 შეტყობინებას დომინიკს. პირველი შეტყობინების შემთხვევაში $Y \rightarrow \Psi(X) \rightarrow Mes_1$ წარმოადგენს მარკოვის ჯაჭვს. ინსტიქტურად იგი გულისხმობს, რომ Mes_1 -ში შესული ინფორმაცია Y -ზე გაიცემა მხოლოდ არაპირდაპირი გზით $\Psi(X)$ -ის საშუალებით. მარკოვი გულისხმობს, რომ $I(\Psi(X);Mes_1) \geq I(\Psi(X);Mes_1|Y)$.

მეორე შეტყობინების შემთხვევაში, Mes_1 ყველასთვის ცნობილია. შედეგად, ცვლადები $\Psi(X)|Mes_1 \rightarrow Y|Mes_1 \rightarrow Mes_2|Mes_1$ ქმნიან მარკოვის ჯაჭვს, და $I(\Psi(X);Y|Mes_1) \geq I(\Psi(X);Y|Mes_1Mes_2)$.

იგივე არგუმენტი ვრცელდება მესამე შეტყობინებაზე; ანუ, ცვლადები $Y|Mes_1Mes_2 \rightarrow \Psi(X)|Mes_1Mes_2 \rightarrow Mes_3|Mes_1Mes_2$ ქმნიან მარკოვის ჯაჭვს და შესაბამისად

$hI(\Psi(X);Mes_3|Mes_1Mes_2) \geq hI(\Psi(X);Mes_3|Y\ Mes_1Mes_2)$.

მარკოვის პროცესის გამოყენებით პირველი და მესამე შეტყობინებების მიმართ, გამოვლენილი ინფორმაცია

$hI(\Psi(X);Mes_1Mes_2Mes_3) = hI(\Psi(X);Mes_1)$

$+ hI(\Psi(X);Mes_2|Mes_1) + hI(\Psi(X);Mes_3|Mes_1Mes_2)$

შეიძლება შეფასდეს ქვედა ზღვირთ, როგორც

$hI(\Psi(X);Mes_1Mes_2Mes_3) \geq HF(\Psi(X)|Y) - HF(\Psi(X)|Y\ Mes_1) + HF(\Psi(X)|Mes_1)$

$- HF(\Psi(X)|Mes_1Mes_2) + HF(\Psi(X)|Y\ Mes_1Mes_2) - HF(\Psi(X)|Y\ Mes_1Mes_2Mes_3)$

$= hI(\Psi(X);Mes_1Mes_2Mes_3|Y) + hI(\Psi(X);Y|Mes_1) - hI(\Psi(X);Y|Mes_1Mes_2).$

მარკოვის პროცესის გამოყენებით მეორე შეტყობინების მიმართ, ჩვენ ვიღებთ

$hI(\Psi(X);Mes_1Mes_2Mes_3) \geq hI(\Psi(X);Mes_1Mes_2Mes_3|Y) = HF(\Psi(X)|Y),$

სადაც ბოლო განტოლება გამომდინარეობს იმ ფაქტიდან, რომ დომინიკს შეუძლია აღადგინოს $\Psi(X)$, Y და $Mes_1Mes_2Mes_3$ -დან გამომდინარე, აქედან, $HF(\Psi(X)|Y\ Mes_1Mes_2Mes_3) = 0$.

$HF(\Psi(X)) - |Mes|/l$ სიდიდის გაზრდა შესაბამისად ფასდება ზედა ზღვრით, როგორც

$HF(\Psi(X)) - |Mes|/l \leq HI(\Psi(X);Y) \leq HI(X;Y).$

შედეგად, შეთანხმების ეფექტურობას განვსაზღვრავთ შემდეგნაირად

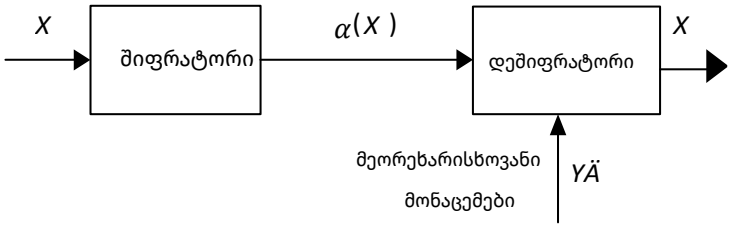
$$\eta = \frac{H(\Psi(X)) - |Mes|/l}{hI(X;Y)}. \qquad (45)$$

ამ თავის დანარჩენი ნაწილი შემდეგნაირად არის ორგანიზებული. პირველად მიმოვიხილავთ მეორეხარისხოვანი მონაცემებით საწყისი კოდირების ზოგად ამოცანას და მოვიყვანთ რამდენიმე ფორმულას. შემდეგ განვიხილავთ არსებულ ორობითი ინტერაქტიული შეთანხმების პროტოკოლებს. დაბოლოს, გაგაცნობთ ტურბო კოდებს და დაბალი -სიხშირის ლუწობის- შემოწმების კოდებს.

6.4 მეორეხარისხოვანი მონაცემებით საწყისი კოდირება

მეორეხარისხოვანი მონაცემებით საწყისი კოდირების ამოცანა მიმღებისთვის არის შემთხვევითი ცვლადის X -ის დაშიფვრა $\alpha(X)$ -ის კოდად, ისე რომ მიმღებს, რომელმაც იცის კორელაციური ცვლადი Y, შეუძლია გაშიფროს $\overline{X} = \beta(\alpha(X), Y)$ რათა აღადგინოს X უშეცდომოდ, $\overline{X} = X$, ან შესაძლოა მცირე შეცდომით, რა შემთხვევაშიც $HPr[\overline{X} = X] \approx 1$. მარტივად რომ ვთქვათ, შემდგომში ჩვენ გვავიწყდება სიტყვები „მიმღებთან“ , რადგან არასოდეს განვიხილავთ მეორეხარისხოვანი მონაცემების შემთხვევას „გამგზავნთან“. გადამწყვეტი მომენტი ის არის, რომ შიფრატორს არ აქვს წვდომა Y ცვლადზე.

მან იცის XY -ის ერთობლივი განაწილება, მაგრამ არ იცის Y-ის შედეგის მნიშვნელობა როცა შიფრავს X -ის შედეგს.



ნახაზი 12. საწყისი კოდირება.

X -ის საწყისი კოდირება მეორეხარისხოვანი მონაცემებითY, რომელიც ცნობილია დეშიფრატორისთვის როგორც სლეპიანმა და ვულფმა დაამტკიცეს, საწყის კოდირებას მეორეხარისხოვანი მონაცემებით შეუძლია შეკუმშოს წყარო იმ კოეფიციენტით, რომელიც HF(X|Y) -ზე დაბალი არაა. ეს გასაკვირი დადგენილებაა, რადგან ჩანს, რომ შიფრატორისთვის Y -ზე მიუწვდომლობა, ზიანს არ აყენებს დაშიფვრის სიჩქარეს. შიფრატორმა რომ იცოდეს Y, ის შეძლებდა დაეშიფრა X და Y ერთობლივად HF(X,Y) ბიტების გადაცემის სიჩქარის საშუალებით. მხოლოდ Y -ის დაშიფვრა მიიღებს HF(Y) ბიტს, ტოვებს ასევე HF(X,Y)–HF(Y) = HF(X|Y) ბიტს, X -ში მოცემული ინფორმაციის დასაშიფრად.

პრაქტიკაში, მიუხედავად ამისა, ის ფაქტი, რომ Y უცნობია შიფრატორისთვის, უფრო ართულებს დაშიფვრას, რაც წარმოშობს საინტერესო პრობლემებს.

გამოიყენება რა შეთანხმებისთვის, მეორეხარისხოვანი მონაცემებით საწყისი კოდირება ჩვეულებრივ ორიენტირებულია ცალკეული სიმბოლოების შესწორებაზე. თუმცა, შეცდომების - შესასწორებელი კოდების სინდრომებზე დაფუძნებული ფორმულები უფრო მეტად ორიენტებულია სიმბოლოების ბლოკებზე.

6.5 განმარტებები და მახასიათებლები

ალბათობის მოცემული განაწილებისთვის P_{XY} (x,y), ამბობენ, რომ სიმბოლოები $x,x' \in X$ არის დამაბნეველი $y \in Y$ -ის არსებობის შემთხვევაში, ისე რომ

$$P_{XY}(x,y) > 0 \text{ and } P_{XY}(x',y) > 0.$$

თუ შიფრატორი დაშიფრავს ამგვარ x და x′ ერთი და იგივე კოდური სიტყვით, დეშიფრატორმა β შეიძლება ვერ შეძლოს იმის განსაზღვრა, თუ რომელი მათგანი დაიშიფრა.

კოდი შეიძლება იყოს უშეცდომობის კოდი ან თითქმის - უდანაკარგო კოდი. უშეცდომობის კოდის შემთხვევაში, დეშიფრატორმა ყოველთვის უნდა შეძლოს X -ის აღდგენა უშეცდომოდ, ანუ,

$$HPr[\beta(\alpha(X),Y)=X]=1.$$

თითქმის - უდანაკარგო კოდის შემთხვევაში, დეშიფრატორს უფლება აქვს შეცდომის მცირე ალბათობის დაშვების. გაურკვევლობის ალბათობა განისაზღვრება შემდეგნაირად

$$HP_{hc} = HPr[\beta(\alpha(X),Y) \neq X]. (8.1)$$

ბევრი საინტერესო შემთხვევისთვის, როგორიცაა გაუსიანის ცვლადები, ერთობლივი ალბათობის ფუნქცია HP_{XY} შეიძლება იყოს აშკარად დადებითი ყველა სიმბოლური წყვილისთვის. ამრიგად, ყველა სიმბოლო გაურკვეველია. ეს ნიშნავს იმას, რომ დაშვებულ უნდა იქნას შეცდომის არა - ნულოვანი ალბათობა დეკოდერის მხარეს, რაც საშუალებას მისცემს ზოგიერთ სიმბოლოს ჰქონდეს იდენტური კოდური სიტყვა, თუნდაც გაურკვეველი იყოს. ეს სხვა შემთხვევაში ბიექციურს გახდის α(X), რაც დაკარგავს მეორეხარისხოვანი მონაცემების უპირატესობას. გარდა ამისა, QKD -ის კონკრეტულ შემთხვევაში, ბიექციური დაშიფვრის სქემა სრულიად გამოააშკარავებს X -სს, რაც უგულებელვყოფს კლოდსა და დომინიკს შორის გაზიარებულ მთელ საიდუმლოებას.

მეორეხარისხოვანი მონაცემებით კოდის გადაცემის სიჩქარე განისაზღვრება ჩვეულებისამებრ და ჩამოყალიბდება ასე

$R = \sum_x HP_X(x)|\alpha(x)|$. გაითვალისწინეთ, რომ სიჩქარე დამოკიდებულია მხოლოდ მარგინალურ განაწილებაზე X

ალონი და ორლიცკი განსაზღვრავენ ორი სახის ნულოვანი - შეცდომის კოდს: შეზღუდული შემავალი (IR) კოდები და შეუზღუდავი შემავალი (IU) კოდები. რომ განვმარტოთ, შეცდომა შეუძლებელია IU და IR კოდებით, ვინაიდან ორიდან არც ერთი გაურკვეველი სიმბოლო არ განისაზღვრება პრეფიქსულ ან თანაბარ კოდურ სიტყვებზე. ჩვენ ვამატებთ მესამე სახის, კერძოდ , თითქმის - უდანაკარგო შეუზღუდავ შემავალ (NLIU) კოდებს. საკმაოდ უცნაურია, მაგრამ IU კოდები უფრო მეტად შეზღუდულია ვიდრე RI კოდები.

- კოდი α არის IR კოდი თუ α(x) არ წარმოადგენს α(x′) -ის პრეფიქსს მაშინ როცა x და x ′ გაურკვეველია.
- კოდი α არის IU კოდი თუ α(x) ≠ α(x′) მაშინ როცა x და x′′ გაურკვეველია და თუ ყველა შემთხვევისთვის x,x′ ∈ X, α(x) არ წარმოადგენს α(x′) -ის სათანადო პრეფიქსს (მაშინაც კი თუ x და x′ არ არის გაურკვეველი).
- კოდი α არის NLIU კოდი თუ ყველა შემთხვევისთვის x,x′ ∈ X, α(x) არ წარმოადგენს α(x′) -ის სათანადო პრეფიქსს.

ზოგადად, თანმიმდევრული შესასვლელი კოდები ერთიანდება რათა შექმნას ორობითი ნაკადი, ისე რომ უნდა დავრწმუნდეთ, რომ α -თი წარმოქმნილი ნაკადი სათანადაოდ განისაზღვროს. საბედნიეროდ, IR კოდის განმარტება უზრუნველყოფს იმას, რომ α არის უპრეფიქსო კოდი, როცა მოცემულია სიდიდე Y. IR კოდის შემთხვევაში, დამკვირვებელს, რომელსაც არ აქვს წვდომა Y -ზე, შეიძლება ვერ შეძლოს კოდური სიტყვების განსაზღვრა ნაკადში. IU და NLIU კოდების შემთხვევაში, კოდური სიტყვები შეიძლება განისაზღვროს Y -ის ცოდნის გარეშე.

თითქმის უდანაკარგო კოდირებისთვის, შეიძლება დაგვჭირდეს ისეთი კოდების შექმნა, რომლებიც იდენტურ კოდურ სიტყვებს არ ანიჭებს გაურკვეველ სიმბოლოებს. ეს რა თქმა უნდა იწვევს დეკოდირების შეცდომებს, მაგრამ საშუალებას გვაძლევს შევამციროთ სიჩქარე. თუმცა მნიშვნელოვანია თავიდან ავიცილოთ ისეთი კოდური სიტყვა, რომელიც

წარმოადგენს მეორე კოდური სიტყვის სათანადო პრეფიქსს ორი გაურკვეველი სიმბოლოსთვის. დავუშვათ x და x′ გაურკვეველი სიმბოლოებია. თუ α(x) არის α(x′) -ის სათანადო პრეფიქსი, მაშინ |α(x)| ≠|α(x′)| და დეკოდერი ვეღარ შეძლებს კოდური სიტყვის სიგრძის განსაზღვრას. შედეგად, დეკოდერი β დესინქრონიზდება, რაც დანარჩენი ნაკადის გაშიფვრას შეუძლებელს გახდის. NLIU კოდის გამოყენება წარმოადგენს შესაძლო ვარიანტს თითქმის - უდანაკარგო კოდირებისთვის, რადგან კოდის განსაზღვრა შესაძლებელია მეორეხარისხოვანი მონაცემების გარეშეც. გაურკვევლობას შეიძლება მაინც ჰქონდეს ადგილი, მაგრამ დისინქრონიზაცია შეუძლებელია მოხდეს.

IU და NLIU კოდები ორ - ხარისხიანი დაშიფვრის პროცედურის ექვივალენტურია. პირველი, სიმბოლოთა X სიმრავლე წარმოდგენილია უფრო მცირე სიმრავლეზე ამ ფუნქციის საშუალებით: φ:X→**N**:x→φ(x). მაშინ, φ(X) -ით წარმოქმნილი სიმბოლოები დაიშიფრება უდანაკარგო უპრეფიქსო კოდის საშუალებით α_0. ფუნქცია φ(x) ყოფს სიმბოლოებს x ∈ X თანაბარ კოდურ სიტყვათა სიმრავლეებად. შედეგად მიღებული კოდი არის უშეცდომობა თუ რომელიმე ორი გაურკვეველი სიმბოლოსთვის x და x′ ჩვენ გვაქვს φ(x) ≠φ(x′).

(NL)IU კოდის დაშიფვრის ნაწილი α_0 შეიძლება იყოს ჰუფმანის კოდირება ან არითმეტიკული კოდირება. წინას შემთხვევაში, სიჩქარე არის $R = \sum_c HP_{\phi(X)}(c)|\alpha_0(c)|$, სადაც, $HP_{\varphi(X)}(hc)$ აღნიშნავს HPr[φ(X)=hc], და ადასტურებს HF(φHP(X)) ≤ R < HF|(φ(|X))+1. მეორეს შემთხვევაში, სიჩქარე ძალიან ახლოსაა შენონის ზღვართან R ≈ HF(φ(X)).

სანამ შემოგთავაზებთ კოდების ფორმულების მაგალითებს, აგიხსნით კავშირს უშეცდომობის შემთხვევასა და ზოგიერთ გრაფიკულ სიდიდეებს შორის.

6.6 უშეცდომობის კოდები და გრაფიკული ენტროპიები

განვმარტავთ გაურკვევლობის გრაფიკს და ავხსნით მის კავშირს მეორეხარისხოვანი მონაცემებით უშეცდომობის საწყის კოდირების ამოცანასთან მიმართებაში. დავუშვათ შემთხვევითი ცვლადებია X და Y. ჩავთვალოთ, რომ G= G(X,Y) არის გრაფიკი ვერტექსის (წვერი) სიმრავლით V(G)=X და კიდეს სიმრავლით EN(G). კიდე {x,x′} ეკუთვნის EN(G) თუ x და x′ გაურკვეველია.

G -ის შეფერილობა წარმოადგენს რუკას φ:V(G) = X → **N** რომელიც ანიჭებს ფერებს წვერებს ისე, რომ ორ მოსაზღვრე წვერს ჰქონდეს სხვადასხვა შეფერილობა. ქრომატული რიცხვი χ(G) არის ფერთა მინიმალური რიცხვი G -ის ნებისმიერ შეფერილობისას. ფერები, რომლებიც იყენებს ზუსტად χ(G) ფერებს უწოდებენ მინიმალურ კარდინალური რიცხვის ფერებს.

ალბათური გრაფიკა წარმოადგენს წყვილს (G,HP), სადაც G არის გრაფა და HP ალბათობის განაწილება მის წვეროებზე. მარტივად რომ ვთქვათ, ასევე ავღნიშნავთ როგორც G(X,Y) ალბათურ გრაფას, რომელიც მიღებულია გაურკვევლობის გრაფადან G(X,Y) და ალბათური განაწილებიდან, რაც დაკავშირებულია შემთხვევით ცვლადთან X.

G(X,Y)-ის φ ფერის ენტროპია არის შემთხვევითი ცვლადის φ(X) ენტროპია HP(φ(X)). G(X,Y)-ის ქრომატული ენტროპია $HF_{\chi}(G(X,Y))$ არის მისი რომელიმე ფერის მინიმალური ენტროპია,

$$HF_{\chi}(G(X,Y)) = \min\{HF(\varphi(X)) : G\text{-ის ფერი } \varphi \}. \qquad (46)$$

დაბოლოს, მინიმალური ენტროპიის ფერი არის φ შეფერილობა, რომელიც აღწევს ქრომატულ ენტროპიას.

ალონმა და ორლიცკიმ გვიჩვენეს, რომ IR კოდის მინიმალური სიჩქარე R_{IR} შეფასებულია ზედა ზღვრით შემდეგნაირად

$$R_{IR} \le H_{\chi}(G(X,Y)) + 1. \qquad (47)$$

და რომ ყველაზე დაბალი ასიმპტომურად მისაღწევი სიჩქარე X -ის მრავალი მაგალითის გადასაცემად IR კოდის გამოყენებით არის $R_{IR,\infty} = \lim_{hd\to\infty} H_{\chi}\left(G^{\wedge Hd}(X,Y)\right)/hd$, სადაც $G^{\wedge hd}$ არის hdth და G -ის ხარისხი. IU

კოდებისთვის, მათ აჩვენეს, რომ მინიმალური სიჩქარე R_{UI} შედარებით დაბალია და შეფასებულია როგორც ზედა ზღვარი შემდეგნაირად

$$HF_{\chi}(G(X,Y)) \leq R_{IU} \leq HF_{\chi}(G(X,Y)) + 1. \quad (48)$$

დაბოლოს, ყველაზე დაბალი ასიმპტომურად მისაღწევი სიჩქარე X -ის მრავალი მაგალითის გადასაცემად UI კოდის გამოყენებით ტოლია $R_{IU,\infty} = \lim_{hd\to\infty} HF_{\chi}\left(G^{vhd}(X,Y)\right)/hd$, რაც წარმოადგენს h_{dth} ან $_G$ -ის ხარისხს.

UI კოდების ორ -ხარისხიანი დაშიფვრის მიდგომა შეიძლება დახასიათდეს პირველ რიგში როგორც G(X,Y) გრაფის ფერი φ და შემდეგ როგორც ფერთა მონაცემების დაშიფვრა α_0. ოპტიმალურ IU კოდებს, კერძოდ, არითმეტიკული კოდირებით, შეუძლია მიაღწიოს იმ სიჩქარეებს, რომლებიც თავისდაუნებურად ახლოსაა $HF_{\chi}(G(X,Y))$ -თან. NLIU კოდებისთვის, მიუხედავად ამისა, φ არ არის უთუოდ

G(X,Y)-ის ფერი, ვინაიდან φ დაშვებულია, რომ ჰქონდეს $\varphi(x) = \varphi(x')$ მაშინაც კი როცა x და x′ გაურკვეველია, ანუ, როცა $\{x,x'\} \in E(G)$.

შეიძლება მაცდუნებელი იყოს ქრომატული ენტროპიის დაკავშირება ცნობილი მინიმალური კარდინალური რიცხვის შეფერილობის ამოცანასთან. მაგალითად, ვითსენჰაუსენი უშეცდომობის კოდებს უკავშირებს გაურკვევლობის გრაფიკის ქრომატულ რიცხვს. მიუხედავად ამისა, ნაჩვენები იქნა, რომ მინიმალური კარდინალური რიცხვის შეფერილობა უეჭველი არ ნიშნავს საუკეთესო მაჩვენებელს. ქრომატული რიცხვი და ქრომატული ენტროპია სინამდვილეში საკმაოდ განსხვავებული ამოცანებია.

კომპლექსურობა: მინიმალური ენტროპიის ფერის პოვნა NP რთულია.

თეორემა 11. G(X,Y) გრაფის მინიმალური ენტროპიის ფერის პოვნა NHP-რთულია მაშინაც კი თუ X აქვს ერთგვარი განაწილება, G(X,Y) არის პლანარული და მოცემულია G(X,Y) -ის მინიმალური კარდინალური რიცხვის ფერი. შედეგი ისაა, რომ ოპტიმალური უშეცდომობის კოდების პოვნა რთული ამოცანაა. თუ ასე არ არის HP=NHP, მინიმალური ენტროპიის

ფერის პოვნა გამოიხატება სანიმუშო ფუნქცია |X| -ში. ასე რომ, პრაქტიკაში უმჯობესია მიახლოებითი პასუხები.

მაგალითი: მაგალითის სახით, დავუშვათ X და Y ცვლადები, სადაც X = $\{x_1,x_2,x_3,x_4,x_5\}$ და Y = $\{y_1,y_2,y_3\}$. ალბათობის განაწილება HP_{XY} (x,y) განსაზღვრულია ცხრილში 8.1.

ცხრილი 8.1. საერთო ალბათობის $hp_{XY}(x,y)$ სპეციფიკაცია. ცარიელი ჩანაწერი ნიშნავს, რომ ალბათობა არის ნული.

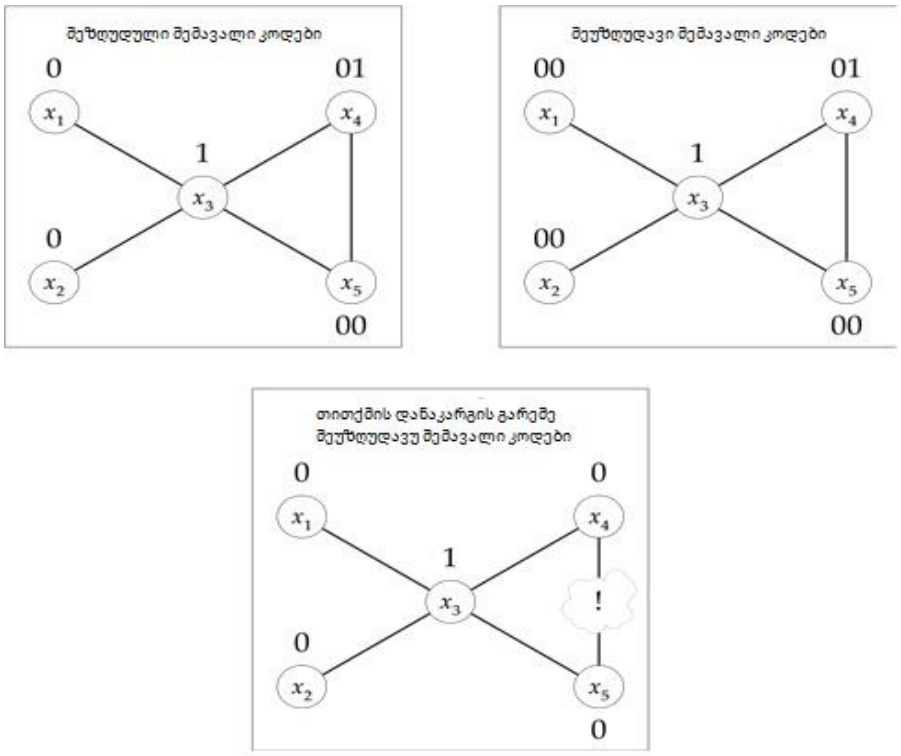
	x_1	x_2	x_3	x_4	x_5
y_1	1/7		1/7		
y_2		1/7	1/7		
y_3			1/7	1/7	1/7

ალბათობის ამ განაწილებით, სიმბოლოები x_1 და x_3 გაურკვეველია, რადგან დეკოდერმა (დეშიფრატორი) უნდა შეძლოს მათი გარჩევა როცა $Y=y_1$. ანალოგიურად, x_2 და x_3 გაურკვეველია და $\{x_3,x_4,x_5\}$ -ის ნებისმიერი წყვილი ასევე შეიცავს გაურკვეველ სიმბოლოებს.

პირველი, რომ IR კოდი არ არის გლობალურად უპრეფიქსო, რადგან მაგალითად სიმბოლოები x_2 და x_5 აისახება კოდურ სიტყვებზე 0 და 00, შესაბამისად. თუმცა, კოდი არის უპრეფიქსო გაურკვეველი სიმბოლოების ნებისმიერი წყვილისთვის. ამ კოდის სიჩქარე არის $R_{RI} = 1 \times 5/7 + 2 \times 2/7 = 9/7$ ბიტი. შემდეგ, UI კოდის მაგალითი ასევე ასახულია. ვინაიდან IU კოდი გლობალურად უნდა იყოს უპრეფიქსო, სიმბოლოები x_1 და x_2 ამჯერად დაკავშირებულია კოდურ სიტყვასთან 00. ამ კოდის სიჩქარე უფრო მაღალია ვიდრე IR კოდის, რადგან IR კოდები უფრო შეზღუდულია, $R_{IU} = 1 \times 3/7 + 2 \times 4/7 = 11/7$ ბიტი.

დაბოლოს, ნახაზი 13 ასევე შეიცავს NLIU კოდის მაგალითს. კოდი არის გლობალურად უპრეფიქსო, მაგრამ გაურკვეველი სიმბოლოები x_4 და x_5 დაკავშირებულია ერთი და იგივე კოდურ სიტყვასთან. თუ ჩავთვლით, რომ

დეკოდერი β იღებს თავისუფალ გადაწყვეტილებას, რომ გაშიფროს 0 როგორც x_4 როცა $Y = y_3$, შეცდომის ალბათობა არის $HP_{hc}=HP_{XY}(x_5,y_3) = 1/7$. ამ დაშვებული შეცდომით, სიჩქარე არის ყველაზე დაბალი ამ სამი მაგალითიდან სადაც $R_{NLIU} = 1$ ბიტი.



ნახაზი. 13. გაურკვევლობის გრაფიკი G(X,Y) და კოდების მაგალითები.

6.7 არსებული კოდის ფორმულები

ამჯერად მიმოვიხილავთ რამდენიმე მეთოდს რათა ჩამოვაყალიბოთ უშეცდომო და თითქმის უდანაკარგო კოდები.

ზოგადი ფორმულები: ჟაო და ეფროსი გვთავაზობენ ფორმულას, სახელწოდებით მრავალჯერადი წვდომის საწყისი კოდი (MASC) რათა აწარმოონ ოპტიმალური IR კოდები, რაც ახდენს ჰუფმანის ტიპის და არითმეტიკული ტიპის კოდების გენერალიზებას. მათ შემოაქვთ გამყოფი ხეების ცნება რათა წარმოადგინონ მოთხოვნები, რომლის საფუძველზეც სიმბოლოებს შეიძლება ჰქონდეს თანაბარი ან პრეფიქსი კოდური სიტყვები. IR კოდებისთვის, ხეს შეიძლება ჰქონდეს რამდენიმე დონე; თუმცა IU კოდებისთვის, გამყოფი ხე არის ბრტყელი, რადგან კოდური სიტყვები

შეიძლება არ წარმოადგენს სხვების სათანადო პრეფიქსებს. გამყოფი ხის პოვნა, რომელსაც მივყავართ ოპტიმალურ კოდამდე, რთულია. მიუხედავად ამისა, მოცემული გამყოფი ხისთვის, ოპტიმალური კოდის პოვნა, რომელიც შეესაბამება გამყოფ ხეს, მარტივია.

იგივე ავტორები გვთავაზობენ სწრაფ სუბ- ოპტიმალურ ალგორითმებს, რომლებიც დაფუძნებულია შეზღუდული-თანმიმდევრობის გამყოფებზე. იდეა მდგომარეობს იმაში, რომ დადგინდეს O(X) თანმიმდევრობა X -ის სიმბოლოებზე. დაყოფას შეუძლია მხოლოდ თანამიმდევრული სიმბოლოების შეკრება ისე რომ შეზღუდოს დაყოფების რიცხვი ოპტიმალური კოდის ძიებისას. შეზღუდულია რა მოცემული მიმდევრობით O(X), მათ ალგორითმს შეუძლია ოპტიმალური გამყოფის და მასთან დაკავშირებული კოდის პოვნა $O(|X|^4)$ -ში. კარგი კოდის საპოვნელად სრულდება O(X) -ის ოპტიმიზაცია იმიტირებული ანელირების ან სხვა ევრისტიკული ძიების ალგორითმების გამოყენებით. გლობალური განხორციელება არის $O(|X|^6)$.

„ხარბი“ შერწყმის ალგორითმი, რომელიც სიჩქარის - არეულობის ოპტიმაზაციის მეთოდებისგან გამომდინარეობს, შემოთავაზებულია-ში. მისი კომპლექსურობა არის $O(|X|^3|Y|)$.

უშეცდომობის კოდების დამატებითი თვისებები მოცემულია იანის და ბერგერის მიერ, სადაც უზრუნველყოფილია საჭირო ან საკმარისი პირობები კოდური სიტყვის სიგრძეზე მცირე მეორეხარისხოვანი მონაცემების ანბანის სიდიდეებისთვის და კოულგის, ტუნცელის და როუზის მიერ მოცემულია ინფორმაცია მისაღწევი სიჩქარის კომპონენტის თეორიულ თვისებებზე.

უშეცდომობის კოდის ფორმულები შეიძლება გამოყენებულ იქნას თითქმის - უდანაკარგო კოდების შესაქმნელად. ეს შეიძლება განხორციელდეს უშეცდომობის ფორმულის გამოყენებით მოდიფიცირებულ ერთობლივი ალბათობის განაწილებაზე, სადაც მცირე ზომის ჩანაწერები დადგენილია ნულზე და დანარჩენი ჩანაწერები ხელახლა ნორმირდება.

ეს ხორციელდება პირდაპირი ფორმით. პირველ რიგში, ჩამოთვლილია ერთობლივი ალბათობის განაწილებაში არსებულ ჩანაწერთა ყველა ქვეჯგუფი, რომლებიც აკმაყოფილებს მოცემულ შეზღუდვას გაურკვევლობის ალბათობაზე. შემდეგ, თითოეული ამ ქვეჯგუფისთვის შექმნილია უდანაკარგო MASC მოდიფიცირებული ერთობლივი ალბათობის განაწილებით, როგორც შესასვლელი. დაბოლოს, შერჩეულია შიფრატორი მინიმალური სიჩქარით. მიუხედავად იმისა, რომ ეს მიდგომა იწვევს ოპტიმალურ კოდს გაურკვევლობის საჭირო მაქსიმალური ალბათობისთვის, ასეთი ფორმულა არ არის პრაქტიკული. ევრისტიკა შეიძლება გამოყენებულ იქნას ძიების დასაჩქარებლად, R სიჩქარის გაზრდის ან გაურკვევლობის ალბათობის HP_{hc} ხარჯზე.

6.8 გრაფიკებზე დაფუძნებული ფორმულები

კოულგი, ტუნცელი, რეგუნათანი და როუზი გვიჩვენებენ გაურკვევლობის გრაფებზე დაფუძნებულ IU და IR კოდების ექსპონენციალური - დროის ოპტიმალური დიზაინის ალგორითმს. ისინი განიხილავენ სიმბოლო X სიმრავლის ქვეჯგუფებით ინდუცირებულ ქვეგრაფებს. ოპტიმალური IU და IR მაჩვენებლები რეკურსიულად დაკავშირებულია ინდუცირებულ ქვეგრაფებთან.

იგივე გუნდი გვთავაზობს მრავალწევრიან, თუმცა სუბოპტიმალური დიზაინის ალგორითმს კარგი IU კოდებისთვის, რომელიც დაფუძნებულია გრაფიკის სავარაუდო ფერებზე. იგი იყენებს ფერად ალგორითმს, რომელიც იძლევა ოპტიმალურთან - დაახლოებულ შედეგებს ქრომატული რიცხვის მიმართ, და შემდეგ შიფრავს ფერებს ჰუფმანის კოდის გამოყენებით.

6.9 სინდრომებზე დაფუძნებული ფორმულები

აქამდის, კოდების ყველა ფორმულა ორიენტირებული იყო ცალკეული სიმბოლოების კოდირებაზე. სინდრომებზე დაფუძნებული კოდების ფორმულით, კოდირება ამჯერად დაამუშავებს X სიმბოლოების Hd ბლოკს.

კლოდისთვის დომინიკზე ინფორმაციის გადაცემის გზა X -ის შესახებ არის წრფივი შეცდომის შესწორების კოდის α(X)=HFX სინდრომის გაგზავნა, სადაც X გამოსახულია ზოგიერთ ვექტორულ სივრცეში $GF(q)^{hd}$ და HF კოდის ლუწობის შემოწმების მატრიცაში. ξ = HFx-ის მიღებისას X-ის x შედეგისთვის, დომინიკი ეძებს ყველაზე სავარაუდო $\bar{x}$ პირობითად Y=y-ზე, ისე რომ $HF\bar{x}$= ξ.

დაშიფვრა და გაშიფვრა ასეთ ფორმულებში მომდინარეობს კოდირების თეორიის სტანდარტული მეთოდებიდან. ეს მეთოდი თავისთავად ისეთი მნიშვნელოვანია, რომ ასეთი ფორმულების ორ მაგალითს მოგიყვანთ 8.4 და 8.5 ნაწილებში.

6.10 ორობითი ინტერაქტიული შეცდომის გასწორების პროტოკოლები

ორობითი ინტერაქტიული შეცდომის გასწორების პროტოკოლები ტრადიციულად გამოიყენება QKD -თვის, რომელიც ქმნის ორობითი გასაღების ელემენტებს. ისინი ასევე მნიშვნელოვანია ზოგადად შეთანხმებისთვის, როცა შერწყმულია დაყოფილი შეცდომის გასწორებასთან აქ წარმოგიდგენთ არსებულ პროტოკოლებს ლოგიკური მიმდევრობით. X და Y არის l-ბიტის შემთხვევითი ცვლადები $X,Y \in GF(2)^l$.

6.11 ბენეტი - ბესეტი - ბრასარდი - სალვაილი - სმოლინი

პირველი ორობითი ინტერაქტიული შეცდომის გასწორების (IEC) პროტოკოლი, რომელიც გამოიყენება QKD -ის მოქმედების სფეროში, შექმნა ბენეტმე და მისმა თანამშრომლებმა (BBBSS). იგი მუშაობს გრძელ ორობით მწკრივზე და მოითხოვს, რომ კლოდმა და დომინიკმა გაცვალონ მათი ბიტების ქვეჯგუფის პარიტეტები, სახელწოდებით ქვე ბლოკები. გამყოფი პარიტეტების არსებობა ეხმარება კლოდს და დომინიკს ყურადღება გაამახვილონ შეცდომებზე ბისექციის (შუაზე გაყოფა) გამოყენებით და შეასწორონ ისინი. BBBSS იყენებს რამდენიმე გამეორებას, რომელთა შორისაც ბიტების პოზიციების გადანაცვლება ხდება ფსევდო - შემთხვევითი გზით.

თითოეული გამეორებისას, კლოდი და დომინიკი ყოფენ მწკრივს (დაახლოებით) თანაბარი სიგრძის ქვე ბლოკებად, რომელიც წოდებულია როგორც ქვე ბლოკები. მარტივად რომ ვთქვათ, ჩავთვალოთ, რომ l = nmhw ზოგიერთი მთელი რიცხვისთვის nm და hw. l- ბიტიანი მწკრივები X და Y იყოფა hw-ბიტიან ქვე ბლოკებად. პირველი გამეორებისას, ქვე ბლოკები არის ინდექსების სიმრავლეები $HB_j^{(1)} = \{(j-1)hw + 1 \ldots jhw\}$, $1 \le j \le nm$ -თვის. მომდევნო გამეორებების შემთხვევაში, კლოდი და დომინიკი თანხმდებიან შემთხვევითად - შერჩეულ გადანაცვლებაზე $\pi^{(i)}$. ქვე ბლოკები შეიცავენ ინდექსებს

$$HB_j^{(i)} = \left\{\pi_t^{(i)} : (j-1)hw + 1 \le t \le jhw\right\}. \quad (49)$$

თითოეული ამ ქვე ბლოკის პარიტეტები იცვლება. i, გამეორების შემთხვევაში, კლოდი და დომინიკი ამჟღავნებენ პარიტეტებს

$$\xi_{X,j}^{(i)} = \sum_{t \in HB_j^{(i)}} X_t \text{ and } \xi_{Y,j}^{(i)} = \sum_{t \in HB_j^{(i)}} Y_t \quad (50)$$

შესაბამისად. როდესაც ქვე ბლოკი $HB_j^{(i)}$ არის ისე რომ $\xi_{X,j}^{(i)} \neq \xi_{Y,j}^{(i)}$, ეს ნიშნავს, რომ ქვე ბლოკში არის შეცდომათა კენტი რიცხვი, სულ მცირე ერთი. ასეთ შემთხვევაში იწყება ბისექცია (შუაზე გაყოფა): კლოდი და დომინიკი ცვლიან ნახევარი ქვე ბლოკის პარიტეტს. თუ პარიტეტი არასწორია, ისინი განაგრძობენ ბისექციას აღნიშნული ქვე ბლოკის ნახევარში; სხვა შემთხვევაში, მინიმუმ ერთი შეცდომა მაინც არის ქვე ბლოკის მეორე ნახევარში და ბისექცია ფოკუსირებულია მეორე ნახევარზე. გაყოფა მთავრდება როცა იგი შემოსაზღვრავს მცდარ ბიტს. ამ ბიტის პოზიციის ცოდან საკმარისია დომინიკისთვის, რომ გაასწოროს იგი: მას შეუძლია უბრალოდ გადაატრიალოს ის.

6.12 კასკადი

კასკადი არის BBBSS-ზე დაფუძნებული IEC, მაგრამ გაუმჯობესებული ეფექტურობით, გამოვლენილი ბიტების რაოდენობის თვალსაზრისით. იგი

იყენებს ოთხ გამეორებას. კასკადის პირველი გამეორება BBBSS -ის პირველი გამეორების იდენტურია, მაშინ როცა მომდევნო სამი განსხვავებულია.

BBSSS -გან განსხვავებით, კასკადი თვალყურს ადევნებს ყველა შესწავლილ ქვე ბლოკს და სარგებლობს ამ მონაცემებით, რომელიც გამომდინარეობს მეორე გამეორებიდან. უფრო ზუსტად რომ ვთქვათ, კასკადი ფლობს ქვე ბლოკის ორ სიმრავლეს: HB_0 , ქვე ბლოკები რომლისთვისაც პარიტეტი არის თანაბარი კლოდსა და დომინიკს შორის, და HB_1, ქვე ბლოკები გამყოფი პარიტეტებით. თითოეული ქვე ბლოკი HB რომლისთვისაც პარიტეტი გამოვლინდა (მათ შორის ბისექციის დროს) მოცემულია HB_0 ან HB_1 -ში.

როდესაც ბისექცია სრულდება და შეცდომა სწორდება (ვთქვათ, რომ ბიტი Hb გადატრიალებულია), კლოდი და დომინიკი ათვალიერებენ ყველა ქვე ბლოკის ჩამონათვალს, რომლისთვისაც მათ უკვე გამოითვალეს პარიტეტი მიმდინარე და წინა გამეორებებში. ნებისმიერი ქვე ბლოკი, რომელიც შეიცავს ბიტს Hb ახლა აღიქვავს მის პარიტეტს გადატრიალებულად Hb -ის გასწორების გამო. აქედან გამომდინარე, შეიძლება არსებობდეს ქვე ბლოკები, რომლისთვისაც პარიტეტი თანაბარი იყო კლოდსა და დომინიკს შორის და ახლა უკვე განსხვავებულია. დავუშვათ $\Delta_{hs} \subseteq Bhs$, $hs = 0,1$, არის ქვე ბლოკების სიმრავლე HBhs -ში, რომელიც შეიცავს ბიტს b. ქვე ბლოკების სიმრავლეები განახლებულია შემდეგნაირად:

$$HB_0 \leftarrow HB_0 \setminus \Delta_0 \cup \Delta_1, HB_1$$

$$HB_1 \leftarrow HB_1 \setminus \Delta_1 \cup \Delta_0.$$

გამეორების დასრულებამდე, კლოდი და დომინიკი ასწორებენ ყველა ცნობილ გამყოფ პარიტეტებს. HB_1 -ში არსებულ ყველა ქვე ბლოკს შორის, კლოდი და დომინიკი აგრძელებენ ბისექციას ამგვარ ყველაზე მცირე ქვე ბლოკებში. როცა პოულობენ გასასწორებელ შეცდომას, ისინი კვლავ ანახლებენ ყველა წინა ქვე ბლოკის პარიტეტებს, ანახლებენ HB_0 და HB_1 და იმეორებენ ამ პროცესს მანამ სანამ არც ერთ ნაცნობ ქვე ბლოკს არ ექნება გამყოფი პარიტეტი, ე.ი. სანამ $HB_1 = ?$.

კასკადის მიზანია გამოავლინოს რაც შეიძლება ცოტა პარიტეტი. ამ პერსპექტივით, ქვე ბლოკის სიდიდის hw ალტერნატივა ჩანს, რომ კრიტიკულ როლს თამაშობს. თუ ქვე ბლოკის სიდიდე hw არის დიდი, ვთქვათ ბევრად უფრო დიდია ვიდრე 1/e, სადაც $e=HPr[X_i]\neq Y_i]$ არის ბიტური შეცდომების სიხშირე, შეცდომათა დიდი რაოდენობა, საშუალოდ, შესულია ამ ქვე ბლოკში. ვინაიდან ბისექციას შეუძლია გაასწოროს მხოლოდ ერთ ერთი მათგანი, გამეორება არ იქნება ეფექტური. მეორეს მხრივ, პატარა ქვე ბლოკის სიდიდე (ე.ი. ბევრად მცირე ვიდრე 1/e) ხშირად არ შეიცავს შეცდომას. როდესაც კლოდი და დომინიკი ავლენენ ξ_X და ξ_Y პარიტეტებს, ისინი ვერ იღებენ ბევრ ინფორმაციას რადგან $\xi_X = \xi_Y$ ხდება ხშირად, ან სხვაგვარადაა დადგენილი, $hf(Pr[\xi_X \neq \xi_Y]) \ll 1$. მომსმენი, მეორეს მხრივ, იღებს ინფორმაციას ყოველ გამოვლენილ პარიტეტზე. იდეალური სიტუაცია იქნებოდა, რომ hw ისე იყოს, რომ ქვე ბლოკი შეიცავდეს შეცდომათა საშუალო რაოდენობას მაშინ როცა $hf(Pr[\xi_X \neq \xi_Y]) \approx 1$.

კასკადში, ქვე ბლოკის სიდიდე შეიძლება არჩეულ იქნას ყოველ გამეორებაზე. ქვე ბლოკის სიდიდეები hw_i, $i=1...4$ უნდა შეირჩეს ისე რომ გლობალურად გამოვლინდეს ბიტების მინიმალური რაოდენობა კასკადის განხორციელებისას, და ამავდროულად დასარულს მიღწეულ იქნას შეცდომის ყველაზე მცირე შესაძლო ალაბათობა კლოდსა და დომინიკს მწკრივს შორის.

ქვე ბლოკის სიდიდე კასკადის თავდაპირველ ვარიანტში არის $hw_1 \approx 0.73/e$ და $hw_i = 2hw_i - 1$. ქვე ბლოკის სიდიდის ოპტიმიზაცია შესრულებულ იქნა ნგუიენის მიერ, რომელიც გვაწვდის ოპტიმალური ქვე ბლოკის სიდიდეთა ჩამონათვალს ბიტური შეცდომების სიხშირის e ფართო სპექტრისთვის.

კასკადის სხვა ოპტიმიზაციები ეხება ორ გამეორებას შორის არსებულ მონაცვლეობას. კასკადში, ყველა შესაძლო გადანაცვლებას შორის, ეს გადანაცვლება არჩეულია ფსევდო - შემთხვევითი გზით. ჩენის [კ. ჩენი, კონფიდენციალური კომუნიკაცია (2001)] და ნგუიენის ნაშრომებში შემოთავაზებულია უკეთესი მონაცვლეობითი მეთოდები, იმისათვის რომ

გავითვალისწინოთ ქვე ბლოკის სტრუქტურა და ვეცადოთ თავიდან ავირიდოთ ორი მცდარი ბიტის მოხვედრა ერთი და იგივე ქვე ბლოკში პირველი ორი (ან ოთხივე) გამეორებისას.

მოდით მოკლედ გავაანალიზოთ კასკადით გაცვლილი პარიტეტების რიცხვი. პროტოკოლის შემდეგ, კლოდმა და დომინიკმა გამოავლინეს RX და RY სიდიდე r×l -ის ზოგიერთი R მატრიცისთვის. ამრიგად მათ დააკავშირეს პარიტეტები, რომელიც გამოთვლილია ბიტის პოზიციების იდენტურ ქვეჯგუფებზე. მატრიცა R და გამოვლენილი პარიტეტების რიცხვი r არ არის წინასწარ ცნობილი, მაგრამ წარმოადგენს სხვადასხვა ბისექციების შედეგს და მოულოდნელად შეხვედრილი გამყოფი პარიტეტების რიცხვისა და პოზიციების ფუნქციაა. თავდაპირველი კასკადისთვის, გაცვლილი პარიტეტების r რიცხვი მოქმედებს დაახლოებით როგორც $r/l \approx (1.1 + e)hf(e)$. ოპტიმიზაცია იძლევა პარიტეტების რიცხვს, რომელიც ახლოსაა

$$r/l \approx (1.0456 + 0.515e)hf(e) + 0.0021. \quad (51)$$

თეორიული ზღვარი არის $hf(e)$.

გაითვალისწინეთ, რომ როცა $e = 25\%$, კასკადი ავლენს იმდენივე პარიტეტულ ბიტს რამდენსაც შეიცავს მწკრივი, შესაბამისად, პოტენციურად ავლენს ყველა მონაცემს.

6.13 ფურუკავა - იამაზაკი

მეორე BBBSS -ზე დაფუძნებული IEC წარმოადგენს პროტოკოლს, რომელიც იყენებს ფურუკავა და იამაზაკის (FY) მიერ შექმნილ სრულყოფილ კოდებს. BBBSS -ის მსგავსად, იგი ასევე იყენებს გამეორების გარკვეულ რაოდენობას მათში ბიტის მონაცვლეობით.

BBBSS -ის მსგავსად, FY ასევე ყოფს ორობით მწკრივს ქვე ბლოკებად. კლოდი და დომინიკი ცვლიან ყველა თავიანთი ქვე ბლოკის პარიტეტებს და ამით განსაზღვრავენ რომელი ქვე ბლოკი შეიცავს შეცდომათა კენტ რიცხვს. ინტერაქტიული ბისექციის გამოყენების ნაცვლად, მცდარი ქვე ბლოკების გასწორება არის ცალმხრივი, კლოდიდან დომინიკის მიმართულებით.

გამყოფი პარიტეტის მქონე თითოეული ქვე ბლოკისთვის, კლოდი უგზავნის დომინიკს მის ქვე ბლოკზე გამოთვლილი სრულყოფილი კოდის სინდრომს. ამ მონაცემებიდან გამომდინარე, დომინიკი ცდილობს გაასწოროს მისი ქვე ბლოკი. (ყურადღება მიაქციეთ სინდრომთან მსგავსებას, რომელიც 8.2.4 ნაწილშია).

სამწუხაროდ, ეს პროტოკოლი ნაკლებად ეფექტურია ვიდრე კასკადი გამოვლენილი ბიტების რაოდენობის თვალსაზრისით. მიუხედავად ამისა, ძირითადი აზრი საინტერესოა და შემდგომში შესწავლილია იდენტურ პრინციპებზე დაფუძნებული უფრო ეფექტური პროტოკოლი.

6.14 Winnow

Winnow–ს პროტოკოლი არის IEC, რომელიც ძალიან ჰგავს FY -ის. გაითვალისწინეთ, რომ Winnow ასევე შეიცავს კონფიდენციალურობის გაძლიერების მსგავს ეტაპს, რომელიც უგულებელყოფს ბიტებს შეცდომის გასწორებისას. თუმცა აქ არ ვითვალისწინებთ ამ ასპექტს. სხვა IEC -ის მსგავსად, იგი იყენებს გამეორებათა გარკვეულ რაოდენობას, მათში ბიტების მონაცვლეობით.

BBBSS, FY და კასკადის მსგავსად, Winnow ასევე ყოფს ორობით მწკრივს ქვე ბლოკებად. კლოდი და დომინიკი ცვლიან ყველა მათი ქვე ბლოკის პარიტეტებს და ამით განსაზღვრავენ რომელი ქვე ბლოკები შეიცავს შეცდომათა კენტ რიცხვს. გამყოფი პარიტეტის მქონე ქვე ბლოკებისთვის, კლოდი დომინიკს უგზავნის მის ქვე ბლოკზე გამოთვლილ ჰემინგის კოდის სინდრომს.

BBBSS და კასკადისგან განსხვავებით, რომლებიც იყენებენ ბისექციას, ქვე ბლოკის გასწორება ჰემინგის კოდის საშუალებით სულაც არ ამცირებს აღნიშნულ ქვე ბლოკში შეცდომების რაოდენობას. Winnow -ში მოცემული ჰემინგის კოდი საშუალებას აძლევს კლოდს და დომონიკს გაასწორონ ერთი შეცდომა. თუ ქვე ბლოკში ერთ შეცდომაზე მეტია, დომინიკის მცდელობამ შეიძლება ნამდვილად გაზარდოს შეცდომების რაოდენობა აღნიშნულ ქვე

ბლოკში. ქვე ბლოკის სიდიდე არჩეულ უნდა იქნას ისე რომ გლობალურად შეამციროს შეცდომათა რაოდენობა.

Winnow -ის ქვე ბლოკის სიდიდეების ოპტიმიზაცია ასევე განახორციელა ნგუიენმა. კასკადისგან განსხვავებით, Winnow -ის გამეორებები ერთი მეორისგან დამოუკიდებელია და ამრიგად შეიძლება შესრულდეს ამომწურავი ძიება დაბალი კომპლექსურობით დინამიური პროგრამირების საშუალებით.

Winnow -ის მნიშვნელობა, როგორც ბიტური შეცდომის სიხშირის ფუნქცია, ისეთ სათანადო მრუდს არ მოიცავს როგორსაც კასკადი. შედეგად, ჩვენ ვეყრდნობით მოცემულ ანალიზებს, რათა გამოვიტანოთ დასკვნები. კასკადი უკეთესად ფუნქციონირებს ვიდრე Winnow ბიტური შეცდომის სიხშირეების მიმართ დაახლოებით 10%-მდე. 10% და 18% შორის Winnow უფრო ეფექტურია. Winnow სათანადოდ არ მოქმედებს 18%-ს ზემოთ, ასე რომ ისევ კასკადი უნდა იქნას გამოყენებული 25% -მდე, რაც წარმოადგენს შეცდომის სიხშირეს რაზეც კასკადიმ უნდა გამოავლინოს მთლიანი მწკრივი რომ შეძლოს ყველა შეცდომის გასწორება.

6.15 კასკადისა და Winnow -ს ინტერაქტიულობა

გვაქვს რა ორი ყველაზე ეფექტური IEC, კასკადი და Winnow, მოდით შევადაროთ მათი სტანდარტები ინტერაქტიულობის თვალსაზრისით.

კასკადსა და Winnow -ს შორის მნიშვნელოვან განსხვავებას წარმოადგენს საჭირო ინტერაქტიულობის დონე. კასკადის განხორციელებისას-სულ მცირე მეორე და უფრო მეტი გამეორებისთვის-კლოდი უნდა დაელოდოს დომინიკისგან პარიტეტულ ბიტს სანამ ის გაიგებს თუ რომელი პარიტეტული ბიტი უნდა გადასცეს, და პირიქით. შეიძლება ისინი ასრულებენ გაყოფას და მათ უნდა მოიცადონ, რათა დაინახონ თანაბარი პარიტეტები აქვთ თუ განსხვავებული, იმისათვის რომ გადაწყვიტონ არსებული ქვე ბლოკის მარცხენა ნახევარზე გააკეთონ აქცენტი თუ

მარჯვენაზე. ამრიგად, თითოეულ მხარეს მხოლოდ ერთი ბიტის გადაცემა შეუძლია ერთ ჯერზე.

ეს ერთ ბიტიანი ინტერაქტიულობა შეიძლება პრობლემად იქცეს პრაქტიკაში. პირველი, გამოყენებული ქსელის სერვისებიდან გამომდინარე, ერთ - ბიტიანი შეტყობინება უნდა შევიდეს ასობით ან ათასობით ბაიტის ბევრად უფრო დიდ შეტყობინებაში. მონაცემთა შეკუმშვის თვალსაზრისით, რთულია უფრო ნაკლებ ეფექტური გავხადოთ იგი. მაშინ, შეტყობინებების რაოდენობა დამოკიდებულია შესათანხმებელი მწკრივის სიდიდეზე. შეტყობინების გადაცემამ შეიძლება განიცადოს მოლოდინის დრო, რომელიც უნდა გამრავლდეს გასაცვლელი პარიტეტული ბიტების რაოდენობაზე. მოლოდინის დრო შესაბამისად l-ის პროპორციულია.

გადაცემის ეფექტურობის ამ დიდი დანაკარგის თავიდან აცილების გზა არის ის, რომ გავყოთ l-ბიტის მწკრივი, რათა მოხდეს მისი შეთანხმება l ბიტის ნაწილებთან, სადაც l არის ფიქსირებული პარამეტრი, მაგალითად., l=10 000. თითოეული ნაწილი შეთანხმებულია კასკადის დამოუკიდებელი მაგალითით, რაც მოითხოვს დაახლოებით v = l/l პროტოკოლის პარალელურ მაგალითებს. ამ მაგალითების შესრულება სინქრონიზებულია იმდაგვარად, რომ v×1 ბიტები შეიძლება გადაიცეს ერთჯერადი შეტყობინებით. შეტყობინებების რაოდენობა და შესაბამისად მოლოდინის დრო, უკვე აღარ არის l -ის პროპორციული.

Winnow -ს შემთხვევა საკმაოდ განსხვავებულია. ყველა ქვე ბლოკის პარიტეტი შეიძლება გადაიცეს ერთი შეტყობინებით, კლოდიდან დომინიკზე და შემდეგ დომინიკიდან კლოდზე. შემდეგ, ყველა მცდარი ქვე ბლოკის ჰემინგის სინდრომი შეიძლება გაიგზავნოს ერთი და იგივე შეტყობინებით კლოდიდან დომინიკზე. ამრიგად Winnow მოითხოვს მხოლოდ სამ შეტყობინებას ყოველ გამეორებაზე, შესათანხმებელი ბიტების რაოდენობისგან დამოუკიდებლად.

6.16 ტურბო კოდები

როდესაც გამოიყენება არხის კოდირებისთვის ან მეორეხარისხოვანი მონაცემებით საწყისი კოდირებისთვის, დადგენილია, რომ ტურბო კოდები აღწევენ ისეთ სიჩქარეს, რომელიც ძალიან ახლოსაა შენონის ზღვართან. ტურბო კოდების კარგი მოქმედება ძირითადად განპირობებულია განმეორებითი „რბილი დეკოდირების“ გამოყენებით, ანუ, იქ სადაც დეკოდირება არა მხოლოდ გაშიფრულ ბიტს აწარმოებს, არამედ მას სანდოობასაც უკავშირებს.

ტურბო კოდებს აქვთ უპრეცედენტო მოქმედება და ბეროუს, გლავიუქსის და თითიმაიშიმას თავდაპირველმა ნაშრომმა დაიწყო რევოლუცია საინფორმაციო თეორიის საზოგადოებაში. ტურბო კოდები ყურადღებით გაანალიზდა და ბევრად გაუმჯობესდა. ასევე, აღმოჩენილ იქნა სხვა სახის ძლიერი კოდები, რომლებიც იყენებენ რბილი დეკოდირების მეთოდებს, როგორიცაა დაბალი -სიხშირის პარიტეტის შემოწმების (LDPC) კოდები, რომელსაც გაგაცნობთ 8.5 ნაწილში.

ამ ნაწილში, მოკლედ გაგაცნობთ ტურბო კოდებს, რომელიც აშკარა ფოკუსირებას აკეთებს მეორეხარისხოვანი მონაცემებით საწყის კოდირებაზე არხის კოდირების ნაცვლად. პირველ რიგში, აგიღწერთ კონვოლუციურ კოდებს, რადგან ისინი შეადგენენ ტურბო კოდების მნიშვნელოვან ინგრედიენტს. შემდეგ, აგიხსნით თუ როგორ შეიძლება ამ კოდების „რბილი-დეკოდირება“. დაბოლოს, ეს ინგრედიენტები შედგენილია ტურბო კოდების შესაქმნელად.

6.17 კონვოლუციური კოდები

ტრადიციული შეცდომის გასწორების კოდებისგან განსხვავებით, რომლებიც მუშაობს კონკრეტული სიდიდის სიმბოლოების ბლოკებზე, კონვოლუციური კოდის შიფრატორი იღებს მის შესასვლელად ბიტების ნაკადს და უშვებს ბიტების ნაკადს. პრაქტიკული მიზეზების გამო, მიგვაჩნია, რომ იგი შიფრავს l- ბიტის მწკრივს, მაგრამ ეს სიდიდე შეიძლება

თავისუფლად განსაზღვროს კოდის მომხმარებელმა კოდის სტრუქტურაში მნიშვნელოვანი ცვლილების გარეშე.

კონვოლუციური შიფრატორი შეიცავს mes -ბიტის მდგომარეობას state hs = ($hs^{(1)}$,...,$hs^{(mes)}$), რომელიც იძენს შემავალი ბიტების ფუნქციას. გამომავალი ნაკადი არის როგორც შემავალი ბიტების ასევე მდგომარეობის წრფივი ფუნქცია. შიფრატორი დროში დამოუკიდებელია და შესაძლებელია აღვიქვათ, როგორც კონვოლუციური ფილტრი GF(2) -ში, მისი სახელიდან გამომდინარე. (გაითვალისწინეთ, რომ კონვოლუციურ შიფრატორს გარკვეული საერთო მსგავსება აქვს ძვრის წრფივ უკუკავშირიან რეგისტრთან).

ჩვენ უფრო კონკრეტულად შემოვისაზღვრებით ორობითი სისტემური რეკურსიული კონვოლუციური კოდებით. ამ მოქმედების არეალში, სისტემატური ნიშნავს, რომ შემავალი ბიტები უცვლელი ჩანს გამომავალ ნაკადში. შიფრატორი რეკურსიულია, იმიტომ რომ მდგომარეობის კონტენტი უკანვე ბრუნდება თავისივე მდგომარეობაში და გამომავალ ნაკადში.

კონვოლუციური კოდის გამოსასვლელი შედგება ბიტის ორი ნაკადისგან: ერთი, რომელიც შეიცავს შემავალ ბიტებს $x_{1...l}$ შეუცვლელს, სახელწოდებით სისტემატიური ბიტები, და მეორე, რომელიც შეიცავს პარიტეტულ ბიტებს $\xi_{1...l}$.

კონვოლუციური კოდი განისაზღვრება ორი მრავალწევრის ფორმალური თანაფარდობით D -ში:

$$G(D) = f(D)/g(D),$$

$$f(D) = f_0 + f_1 D + \cdots + f_{mes} D^{mes},$$

$$g(D) = g_0 + g_1 D + \cdots + g_{mes} D^{mes},$$

სადაც მიჩნეულია, რომ $g_0 = 1$. D სიმბოლო უნდა განვიხილოთ როგორც შეფერხება შიფრატორის მეხსიერებაში. მრავალწევრი f გვიჩვენებს, თუ როგორ წარმოიქმნება პარიტეტული ბიტები მდგომარეობიდან, ხოლო მრავალწევრი g განსაზღვრავს თუ როგორ ვითარდება მდგომარეობა და

როგორ ბრუნდება უკან. როგორც ქვემოთაა დაზუსტებული, კოეფიციენტები f_j და g_j გვიჩვენებს არის თუ არა კავშირი jth ფორმის ბიტიდან პარიტეტამდე და უკუკავშირამდე, შესაბამისად. მეორე პირობითი გზა კონვოლუციური კოდის განსასაზღვრად არის მრავალწევრების შეფასება D=2 და შედეგად მიღებული ორი მთელი რიცხვის თანაფარდობის დაწერა. მაგალითად, ვსაუბრობთ კონვოლუციურ კოდზე 7/5 მოცემული შემთხვევისთვის G(D) = $(1 + D + D^2)/(1 + D^2)$.

მოდით ახლა აღვწეროთ თუ როგორ მუშაობს კონვოლუციური შიფრატორი მოცემული G(D) -თვის. ყოველი მომდევნო შემავალი ბიტისთვის x_t t, $1 \le t \le l$, პარიტეტული ბიტები და მდგომარეობის ბიტები შემდეგნაირად ვითარდება:

$$\xi_t = f_0 x_t + \sum_{j=1\ldots m} f_j hs_{t-1}^{(j)} + f_0 g_{mes} hs_{t-1}^{(mes)}$$

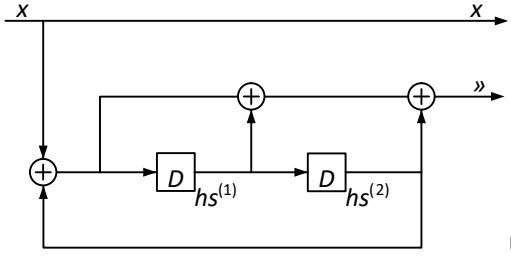
$$hs_t^{(1)} = x_t + \sum_{j=1\ldots m} g_j hs_{t-1}^{(j)}$$

$$hs_t^{(i)} = hs_{t-1}^{(i-1)} \text{ for } 2 \le i \le mes$$

პირველ გამეორებამდე, მდგომარეობა დაყენებულია ნულზე, ანუ, $hs_0^{(j)} = 0$ მოცემული შემთხვევისთვის $1 \le j \le mes$.

ტურბო კოდები და შესაბამისად კონვოლუციური კოდები თავდაპირველად განსაზღვრულია არხის კოდირებისთვის. მეორეხარისხოვანი მონაცემებით საწყისი კოდირებისთვის საჭიროა ორი უმნიშვნელო ადაპტაცია, რომელსაც ახლა ავღწერთ.

პირველი, არხის კოდირება მოითხოვს, რომ ორივე, სისტემატური და პარიტეტული ბიტები გაგზავნილ იქნას არხზე, რადგან მიმღები ორივეს საჭიროებს თავდაპირველი შეტყობინების აღსადგენად.



ნახაზი 14. კონვოლუციური შიფრატორი.

კონვოლუციური შიფრატორის მაგალითი mes=2 ბიტის მეხსიერებით. შიფრატორი განსისაზღვრება $G(D) = (1+D+D^2)/(1+D^2)$ -ით ან 7/5 -ით. არის კავშირები მდგომარეობის ბიტებიდან $hs^{(1)}$ და $hs^{(2)}$ პარიტეტულ ბიტებზე, რადგან გამომთვლელი შეიცავს D და D^2, შესაბამისად. გაითვალისწინეთ, რომ კავშირი არ არის $hs^{(1)}$-დან უკუკავშირამდე, რადგან D -ს კოეფიციენტი მნიშვნელში არის 0.

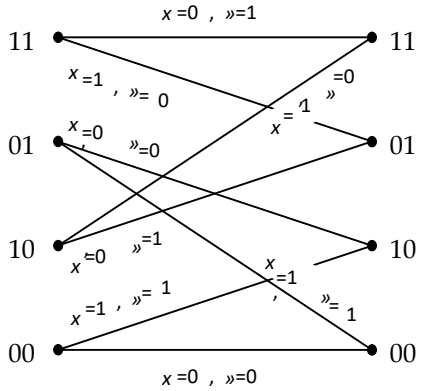
მეორეხარისხოვანი მონაცემებით საწყისი კოდირებისთვის, მიუხედავად ამისა, მხოლოდ პარიტეტული ბიტები იგზავნება მეორეხარისხოვანი მონაცემების სახით (უხმაურო) საჯარო კლასიკურ აუთენტიფიცირებულ არხზე. ბობისთვის სისტემატური ბიტების ხმაურიანი ვარიანტი ცნობილი ხდება Y -ის მეშვეობით, თითქოს X გაგზავნილი ყოფილიყო ხმაურიან არხზე. რა თქმა უნდა, ყველა პარიტეტული ბიტი არ იგზავნება მეორეხარისხოვანი მონაცემების სახით. ვინაიდან მეორეხარისხოვანი მონაცემებით საწყისი კოდირების მიზანია ბიტების ყველაზე მცირე რაოდენობის გაგზავნა, ისე რომ ბობმა შეძლოს X -ის აღდგენა, პარიტეტული ბიტების მხოლოდ კარგად - შერჩეული ქვეჯგუფი ინახება. პარიტეტული ბიტების მოცილების პროცესს ეწოდება წაშლა (puncturing) და მოგვიანებით დავუბრუნდებით ამ საკითხს, როცა ავღწერთ ტურბო კოდებს, ამ სიტყვის ზუსტი გაგებით.

მეორე, როდესაც ტურბო კოდები გამოიყენება არხის კოდირებისთვის, შემავალი მწკრივის დაშიფვრა გამოსცემს დამატებით mes პარიტეტულ ბიტებს $z_{l+1\ldots l+mes}$ შემავალი l ბიტების დაშიფვრის შემდეგ. ეს ბოლო პარიტეტული ბიტები წარმოიქმნება შემავალი ბიტებით, რომლებიც 0-ის ტოლია და არანაირი მდგომარეობის უკუკავშირი არ არის, იმისათვის რომ აიძულოს საბოლოო მდგომარეობა იყოს

$hs=(0,0,\ldots,0)$. ეს აფიქსირებს როგორც საწყის ისე საბოლოო მდგომარეობებს სასაზღვრო მდგომარეობად, რომელსაც ითხოვს დეკოდერი. მეორეხარისხოვანი მონაცემებით საწყისი კოდირების ფარგლებში, ჩვენ

ნაცვლად ამისა, ვთვლით რომ ალისა ავლენს საბოლოო მდგომარეობას როგორც მეორეხარისხოვან მონაცემს, ე.ი. იგი გადასცემს ბობს $\sigma_l = hs_l$. ეს ასევე განსაზღვრავს როგორც საწყის ისე საბოლოო მდგომარეობებს ექვივალენტური, მაგრამ უფრო მარტივი გზით.

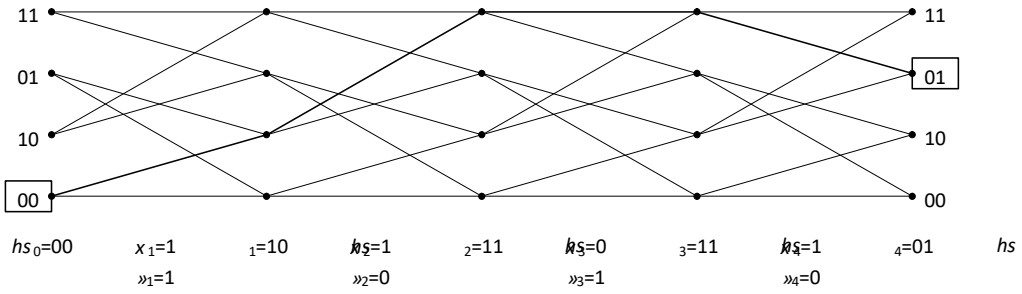
კონვოლუციური კოდების გრაფიკულად წარმოდგენის პოპულარული საშუალება არის დიაგრამის გამოყენება. არაფორმალურად რომ ვთქვათ, ეს დიაგრამა არის ორი ნაწილისაგან შემდგარი გრაფიკი კვანძების ჯგუფით, რომელიც წარმოადგენს 2^{mes} მდგომარეობას t–1 -ზე ან შემავალ მდგომარეობებს, და კვანძების ჯგუფი, რომელიც წარმოადგენს მდგომარეობებს t -ზე, ან გამომავალ მდგომარეობებს. დიაგრამა შედგება კიდეებისგან, რომელიც აკავშირებს hs_{t-1} მდგომარეობას hs_t მდგომარეობასთან, მხოლოდ და მხოლოდ იმ შემთხვევაში თუ იქ არის შემავალი სიმბოლო x_t რომელიც იწვევს მდგომარეობის გადასვლას hs_{t-1} -დან hs_t -ზე. კიდეები მონიშნულია შესაბამისი შემავალი ბიტით x რომელიც იწვევს ამ კონკრეტულ გადასვლას და ასევე მონიშნულია შესაბამისი პარიტეტული ბიტით ჯ რომელიც წარმოადგენს გამოსასვლელს აღნიშნულ გარემოებებში. გაითვალისწინეთ, რომ დაშიფვრა და ასევე დიაგრამა t -გან დამოუკიდებელია. დიაგრამის მაგალითი მოცემულია ნახაზზე 15.-ზე



ნახაზი 15. კონვოლუციური კოდის 7/5 დიაგრამა.

შემავალი მდგომარეობები განლაგებულია მარცხნივ და აღნიშნულია $hs^{(1)}hs^{(2)}$ -ით. გამომავალი მდგომარეობები განლაგებულია მარჯვნივ.

გაითვალისწინეთ, რომ დიაგრამა შესაძლებელია რომ შეერთდეს რათა წარმოადგინოს მდგომარეების გადასვლა hs_0-დან hs_l-ზე. მოცემული შემავალი მწკრივისთვის, მდგომარეობის გადასვლები იკვალავს გზას $hs_0 = 0$ კვანძიდან $hs_l = \sigma_l$ კვანძამდე, რომელიც ილუსტრირებულია ნახაზზე 16.



ნახაზი 16. კონვოლუციური კოდის 7/5 მდგომარეობის გადასვლა

კონვოლუციური კოდის 7/5 მდგომარეობის გადასვლის გზის მაგალითი $l = 4$- ბიტის შემავალი ბლოკისთვის $x_{1\ldots4} = 1101$. საწყისი მდგომარეობა არის $hs_0 = 00$ და საბოლოო მდგომარეობა არის $\sigma_4 = hs_4 = 01$.

თავი 7. კონვოლუციური და ტურბო კოდები.

ახლა როდესაც ავღწერეთ შიფრატორი, მოდით ავღწეროთ თუ როგორ შეუძლია ბობს აღადგინოს X, Y და Ξ -დან. გაითვალისწინეთ, რომ ჯერჯერობით არ ვსაუბრობთ ტურბო კოდებზე, არამედ მხოლოდ კონვოლუციურ კოდებზე. ფაქტიურად, როგორც ტურბო კოდების შემადგენელი ნაწილი, გვსურს Y და Ξ -დან აღვადგინოთ არა მხოლოდ ბიტის სიდიდე არამედ მისი, როგორც ნულის ან ერთის ალბათობის შეფასება. ეს წარმოადგენს „რბილ გაშიფვრას“ რომელსაც მოითხოვს ტურბო კოდები.

მაქსიმალური აპოსტერიორული (MAP) ალგორითმი, რომელიც აქაა აღწერილი, გამოიგონა ბალმა და მისმა თანამშრომლებმა. მიზანი არის თითოეული სიმბოლოსთვის x_t, ვიპოვოთ თუ რომელია ყველაზე სავარაუდო აპოსტერიორი, ანუ, როცა მიღებულ იქნება ყველა სიმბოლო $y_{1\ldots l}$.

რბილი გაშიფვრის შეთანხმებიდან გამომდინარე, ჩვენ ვაფასებთ აპოსტერიორული ალბათობების ლოგარითმის - ალბათობის კოეფიციენტს (LLR), ე.ი.

$$L(X_t \mid y_{1\ldots l}) = \ln \frac{H \Pr[X_t = 0 \mid Y_{1\ldots l} = y_{1\ldots l}]}{H \Pr[X_t = 1 \mid Y_{1\ldots l} = y_{1\ldots l}]} = \ln \frac{H\Pr[X_t = 0, Y_{1\ldots l} = y_{1\ldots l}]}{H\Pr[X_t = 1, Y_{1\ldots l} = y_{1\ldots l}]}$$

$L = L(X_t|y_{1\ldots l})$ -ის მნიშვნელობა დადებითია თუ $X_t = 0$ უფრო მეტად შესაძლებელია ვიდრე $X_t=1$, და პირიქით თუ მნიშვნელობა უარყოფითია. თუ $L=0$ ორივე მნიშვნელობა თანაბრად შესაძლებელია; როცა $X_t = 0$ (or $X_t = 1$) განსაზღვრულია, შესაბამისად გვაქვს $L = +\infty$(ან $L = -\infty$).

მხოლოდ სიმბოლოებზე x_t და $y_{1\ldots l}$ შეხედვის ნაცვლად, ჩვენ ვაფასებთ LLR -ს მდგომარეობის სხვადასხვა გადასვლების ალბათობების გამოთვლით. კერძოდ, ჩვენ განვიხილავთ მდგომარეობის გადასვლას t -ზე, ყველა მარშრუტისთვის, რომელიც მომდინარეობს $hs_0 =0$-დან hs_t-1 -მდე და ყველა მარშრუტი, რომელიც დასაბამს იღებს hs_t -ში და სრულდება $hs_l = \sigma_l$ -ში, hs_t-1 და hs_t -ის ყველა შესაძლო მნიშვნელობებისთვის. LLR შეიძლება ექვივალენტურად გადმოცემულ იქნას როგორც

$$L(X_t \mid y_{1\ldots l}) = \ln \frac{\sum_{hs_{t-1},hs_t,\xi_t} HP(hs_{t-1},hs_t,0,\xi_t)}{\sum_{hs_{t-1},hs_t,\xi_t} HP(hs_{t-1},hs_t,1,\xi_t)}, \quad (52)$$

სადაც $HP(hs_t{-}1,hs_t,x_t,\xi_t)$ არის მოცემული ჩანაწერი ამ ფორმულისთვის

$HP(hst{-}1,hst,xt,\xi t) = HPr[HSt{-}1 = hst{-}1,HSt = hst,Y1\ldots l = y1\ldots l,Xt = xt,\Xi t = \xi t]$.

მოდით პირველ რიგში განვავრცოთ ყველა წევრი და შემდეგ ავღწერთ სხვადასხვა მამრავლებს ერთმანეთის მიყოლებით. ალბათობა $HP(s_t{-}1,s_t,x_t,\xi_t)$ შეიძლება შეიცვალოს და დაიწეროს ამგვარად

$HP(hs_t{-}1,hs_t,x_t,\xi_t) = \alpha_t{-}1(hs_t{-}1)\gamma(hs_t{-}1,hs_t,x_t,\xi_t)\beta_t(hs_t)$,

$\alpha t(st) = HPr[HSt = hst,Y1\ldots t = y1\ldots t]$,

$\gamma(hs_t{-}1,hs_t,x_t,\xi_t) = \delta(hs_t{-}1,hs_t,x_t,\xi_t)HP_Y\,|X(y_t|x_t)HP_X(x_t)HP_\Xi(\xi_t)$,

$\beta_t(hs_t) = HPr[HS_t = hs_t,Y_t{+}1\ldots l = y_t{+}1\ldots l]$,

$\delta(hs_t{-}1,hs_t,x_t,\xi_t) = Pr[HS_t = hs_t,\Xi_t = \xi_t|HS_t{-}1 = hs_t{-}1,X_t = x_t]$.

ფუნქცია $P(hs_t{-}1,hs_t,x_t,\xi_t)$ ჯერ იყოფა სამ მამრავლად. პირველად, ფუნქცია $\alpha_t(hs_t)$ განიხილავს წარსულს და გვამცნობს რამდენად სავარაუდოა რომ შიფრატორი მივიდეს hs_t მდგომარეობამდე, გამომდინარე იქიდან, რომ ჩვენ შევისწავლეთ $y_{1\ldots t}$. შემდეგ, ფუნქცია $\beta_t(hs_t)$ განიხილავს მომავალს და ვინაიდან ვიცით, რომ დეკოდერი მიაღწევს σ_l მდგომარეობას l -ის დროზე, გვაძლევს ალბათობას, რომ ჩვენ დავიწყეთ hs_t მდგომარეობაში t დროზე. დაბოლოს, ფუნქცია $\gamma(hs_t{-}1,hs_t,x_t,\xi_t)$ გვამცნობს რამდენად სავარაუდოა, რომ გადასვლა მოხდეს $hs_t{-}1$ და hs_t შორის t დროზე.

როგორც γ ფუნქციის ნაწილი, $\delta(hs_t{-}1,hs_t,x_t,\xi_t)$ არის ფუნქცია, რომელიც აბრუნებს 1 -ს თუ $hs_t{-}1$ -დან hs_t -ზე გადასვლა გამოცემული პარიტეტით ξ_t არსებობს x_t -თვის როგორც შესასვლელი, და 0 სხვა შემთხვევაში. ასე რომ, რომც შევაჯამოთ ყველა წარსული და მომავალი მდგომარეობა (8.3) განტოლებაში, ეს ფუნქცია δ უზრუნველყოფს, რომ ამოცანაში არჩეულ იქნას მხოლოდ მოქმედი გადასვლები.

ალბათობა $HP_Y\,|X(y_t|x_t)HP_X(x_t) = HP_{XY}\,(x_t,y_t)$ გადამწყვეტია გადასვლისთვის t -დროზე, რადგან იგი პირდაპირ ითვალისწინებს X_t -ის ხმაურიან სიდიდეს,

რომელიც ბობმა მიიღო Y_t -ში. აქ, $HP_X(x_t)$ ცნობილია როგორც აპრიორული ინფორმაცია X_t -ზე.

სიმცირის გამო, $HP_X(x_t) = 1/2$, მაგრამ როგორც უფრო დეტალურად ვიხილავთ, ტურბო კოდების განმეორებითი გაშიფვრა ავრცობს ამ მნიშვნელობას.

გამომდინარე იქიდან წაიშალა თუ არა პარიტეტული ბიტი t დროზე, ალბათობა $HP_Ξ(ξ_t)$ არის ან $HP_Ξ(ξ_t) = ½$ თუ არც ერთი პარიტეტული ბიტი არ მიღებულა ან $HP_Ξ(ξ_t) = 0$ ან 1, მიღებული პარიტეტული ბიტის მნიშვნელობიდან გამომდინარე. (გახსოვდეთ, რომ მეორეხარისხოვანი მონაცემებით საწყისი კოდირების შემთხვევაში, პარიტეტული ბიტები გადაიცემა უდანაკარგოდ). ასე რომ, როცა ცნობილია პარიტეტული ბიტი, განტოლების ჯამი ითვალისწინებს მხოლოდ მდგომარეობის გადასვლებს, რომელიც შეესაბამება მიღებულ პარიტეტულ ბიტს.

რომ შევაჯამოთ, γ ფუნქცია ითვალისწინებს შესაძლო მდგომარეობის გადასვლებს და დამოკიდებულია აპრიორულ ინფორმაციაზე და რეალურ ხმაურიან მნიშვნელობებზე და პარიტეტულ ბიტებზე, რომელიც ბობმა მიიღო. MAP ალგორითმი რომ გავაგრძელოთ, γ ფასდება ყველა დროისთვის $1 \le t \le l$ და ყველა შესაძლო მდგომარეობის გადასვლისთვის. ეს მნიშვნელობები იძლევა ადგილობრივ მონაცემებს მოცემული მდგომარეობის გადასვლის ალბათობაზე მოცემულ დროს. LLR -ის გამოსათვლელად, მიუხედავა ამისა, γ -ის მნიშვნელობები უნდა შეერთდეს, რათა გათვალისწინებულ იქნას ყველა შესაძლო მდგომარეობის გადასვლის მარშრუტის გლობალური სურათი. ეს ისაა, სადაც ასევე საჭიროა α და β ფუნქციები. ფაქტიურად, α და β, ორივე შეიძლება შეფასდეს ეფექტურად რეკურსიული გზით, γ -ის მნიშვნელობების გაერთიანებით სხვადასხვა დროს.

ფუნქცია $\alpha_t(s_t)$ ადასტურებს თვისებას, რომ

$$\alpha_t(\mathrm{hs}_t) = \sum_{\mathrm{x}_t, \xi_t, \mathrm{hs}_{t-1}} \gamma(hs_{t-1}, \mathrm{hs}_t, \mathrm{x}_t, \xi_t)\alpha_{t-1}(\mathrm{hs}_{t-1})$$

$\alpha_t(hs_t)$ -ის მნიშვნელობები ყველა t და hs_t -თვის შეიძლება ამრიგად გამოთვლილ იქნას დაწყებული t = 1-დან, იმ შეთანხმებით, რომ $\alpha_0(0) = 1$ და $\alpha_0(s) = 0$ მოცემული შემთხვევისთვის $hs \neq 0$.

ანალოგიურად, ფუნქცია $\beta_t(hs_t)$ შეიძლება გამოთვლილ იქნას რეკურსიულად დაწყებული ბოლო მდგომარეობიდან. რეკურსია ჩამოყალიბდება შემდეგნაირად

$$\beta_{t-1}(hs_{t-1}) = \sum_{x_t,\xi_t,hs_t} \gamma(hs_{t-1}, hs_t, x_t, \xi_t)\beta_t(hs_t).$$

$\beta_t(hs_t)$ -ის მნიშვნელობები შეიძლება გამოთვლილ იქნას დაწყებული t = l -დან, იმ შეთანხმებით, რომ $\beta_l(\sigma_l) = 1$ და $\beta_l(hs_l) = 0$ მოცემული შემთხვევისთვის $hs_l \neq \sigma_l$.

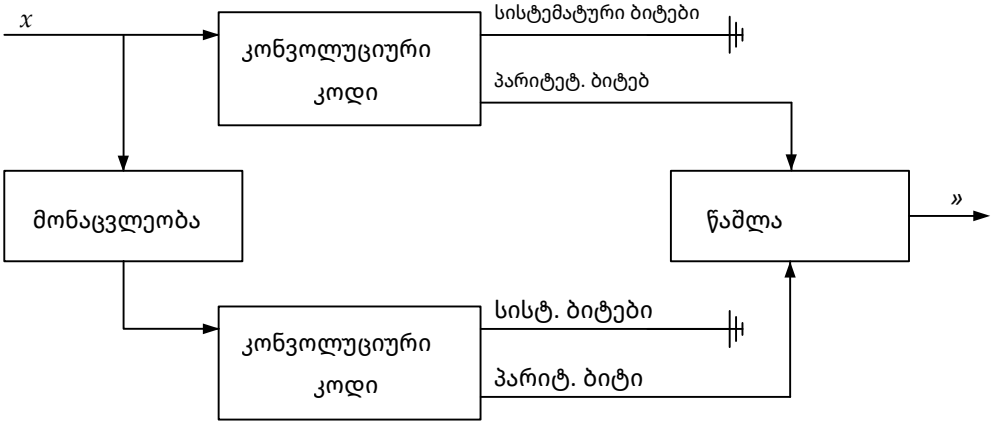
ამჯერად ავღწერთ ტურბო კოდების სტრუქტურას, ამ სიტყვის ზუსტი გაგებით.

7.1 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.

როგორც წესი, მეორეხარისხოვანი მონაცემებით საწყისი კოდირების შემთხვევაში, სისტემატური ბიტები უგულებელყოფილია. ორივე შიფრატორის 2l პარიტეტული ბიტები იშლება რათა შეინარჩუნოს მათგან მხოლოდ ერთი ნაწილი. მოცემული პარიტეტული ბიტების რიცხვი დამოკიდებულია იმ მონაცემებზე, რომელსაც იზიარებენ ალისა და ბობი და ახლოს უნდა იყოს HlHF(X|Y)-თან. გაითვალისწინეთ, რომ არსებობს წაშლის

სხვადასხვა სტრატეგიები, როგორიცაა პარიტეტული ბიტების ფსევდო შემთხვევითი ქვე ჯგუფის გაუქმება.



ნახაზი 17. ტურბო შიფრატორის სტრუქტურა.

ტურბო კოდების გაშიფვრა ეყრდნობა ორივე კონვოლუციური შიფრატორის რბილ დეკოდირებას. ტურბო კოდების კარგი მოქმდება მომდინარეობს იმ ფაქტიდან, რომ თითოეული კონვოლუციური დეკოდერი სარგებლობს მეორის რბილი დეკოდირებით. მოდით ავღწეროთ ეს პროცესი უფრო დეტალურად.

დასაწყისისთვის, პირველი კონვოლუციური კოდი გაიშიფრება MAP ალგორითმის გამოყენებით, პარიტეტული ბიტებით ξ_{CC1} რომელიც წარმოებულია პირველი შიფრატორის მიერ. ეს პროცესი წარმოშობს LLRs $L_1(X_t|y_{1...l})$, $1 \le t \le l$, როგორც 8.4.2 ნაწილშია აღწერილი. პირველი გაშიფვრისთვის, აპრიორული ალბათობები $HP_X(x_t)$ დადგენილია $HP_X(x_t) = ½$ -ზე, ვინაიდან ორივე ბიტი თანაბრად შესაძლებელია.

პარიტეტული ბიტების ξ_{CC2} მეორე დეკოდერში დამუშავებამდე, მიუხედავად ამისა, აპრიორული ალბათობები $HP_X(x_t)$ განისაზღვრება $L_1(X_t|y_{1...l})$ -ის ფუნქციად. ამ გზით, 1 დეკოდერის ცოდნის დონე გადაეცემა 2 დეკოდერს. შემდეგ, 2 დეკოდერის, $L_2(X_t|y_{1...l})$, მიერ წარმოქმნილი LLR გადაეცემა 1 დეკოდერს აპრიორული ალბათობების სახით. პარიტეტული ბიტები ξ_{CC1} შესაბამისად დამუშავდება მეორეჯერ, რაც წარმოშობს უკეთეს შედეგებს, რომლებიც გადაეცემა 2 დეკოდერს და ასე შემდეგ. ეს ალტერნატივა

მეორდება მანამდე სანამ არ მიიღწევა კონვერგენცია ან გამეორებების განსაზღვრულ რაოდენობამდე.

მოდით უფრო ახლოდან შევხედოთ LLR-ს. ფაქტიურად, განტოლების (52) გამომთვლელი და მნიშვნელი შეიძლება მამრავლებად დაიშალოს როგორც

$$\sum_{\mathrm{hs}_{t-1},\mathrm{hs}_t,\xi_t} \mathrm{HP}(\mathrm{hs}_{t-1},\mathrm{hs}_t,\mathrm{x}_t,\xi_t) =$$

$$\left(\sum_{\mathrm{hs}_{t-1},\mathrm{hs}_t,\xi_t} \alpha_{t-1}(\mathrm{hs}_{t-1})\delta(\mathrm{hs}_{t-1},\mathrm{hs}_t,\mathrm{x}_t,\xi_t)\mathrm{hP}_{\Xi}(\xi_t)\beta_t(\mathrm{hs}_t)\right) \times \mathrm{hP}_{\mathrm{Y|X}}(\mathrm{y}_t \mid \mathrm{x}_t) \times \mathrm{hP}_{\mathrm{X}}(\mathrm{x}_t)$$

ამრიგად, LLR შეგვიძლია გავყოთ სამ წევრად,

$$\mathrm{L}(\mathrm{X}_t \mid \mathrm{y}_{1\ldots\mathrm{l}}) = \mathrm{L}_{\mathrm{ext}} + \mathrm{L}_{\mathrm{chf}} + \mathrm{L}_{\mathrm{a-priori}}, \text{ with}$$

$$\mathrm{L}_{\mathrm{ext}} = \ln \frac{\sum_{\mathrm{hs}_{t-1},\mathrm{hs}_t,\xi_t} \alpha_{t-1}(hs_{t-1})\delta(hs_{t-1},\mathrm{s}_t,0,\xi_t)\mathrm{hP}_{\Xi}(\xi_t)\beta_t(\mathrm{s}_t)}{\sum_{\mathrm{hs}_{t-1},\mathrm{hs}_t,\xi_t} \alpha_{t-1}(hs_{t-1})\delta(\mathrm{hs}_{t-1},\mathrm{hs}_t,1,\xi_t)H\mathrm{P}_{\Xi}(\xi_t)\beta_t(\mathrm{hs}_t)}$$

$$\mathrm{L}_{\mathrm{ch}} = \ln \frac{\mathrm{HP}_{\mathrm{Y|X}}(\mathrm{y}_t \mid 0)}{\mathrm{HP}_{\mathrm{Y|X}}(\mathrm{y}_t \mid 1)}$$

$$\mathrm{L}_{\mathrm{a-priori}} = \ln \frac{\mathrm{HP}_{\mathrm{X}}(0)}{\mathrm{HP}_{\mathrm{X}}(1)}$$

LLR, რომელიც მოცემულია როგორც გამოსასვლელი MAP ალგორითმის მიერ ერთი შიფრატორისთვის, შედგება ორი წევრისგან, რომელიც შეიძლება განისაზღვროს ალგორითმის გაშვებამდე: $\mathrm{L}_{\mathrm{chf}}$, რომელიც დამოკიდებულია მხოლოდ X და Y შორის კორელაციებზე (ე.ი. არხზე, არხის კოდირების შემთხვევაში), და $\mathrm{L}_{\mathrm{a\text{-}priori}}$ -ზე, რომელიც მოცემულია MAP ალგორითმის შესასვლელში. ეს ორი წევრი არ გამოიყენება ორ დეკოდერს შორის გაცვლისას.

ამის საპირისპიროდ, ბოლო წევრი $\mathrm{L}_{\mathrm{ext}}$ რომელიც წარმოებულია ერთი შიფრატორის მიერ, შეიცავს მნიშვნელობას, რომელიც დამოკიდებულია მხოლოდ იმ ინფორმაციაზე რაც მეორე დეკოდერისთვის უცნობია და ეწოდება გარეგანი (extrinsic) ინფორმაცია და რომელიც აპრიორული

ალბათობის სახით შეიძლება გადაეცეს მეორე დეკოდერს. 1 დეკოდერის (ან 2 დეკოდერის) MAP ალგორითმის მიერ დაბრუნებული L_{ext} მნიშვნელობიდან გამომდინარე, დეკოდერი 2-ის (ან დეკოდერი 1) აპრიორული ალბათობები განისაზღვრება შემდეგნაირად

$$HP_X(x) = \frac{e^{(-1)^X L_{ext}/2}}{e^{L_{ext}/2} + e^{-L_{ext}/2}} \qquad (53)$$

7.2 დაბალი - სიხშირის პარიტეტული (ლუწობის) - შემოწმების კოდები

დაბალი - სიხშირის პარიტეტული - შემოწმების (LDPC) კოდები პირველად აღმოაჩინა გალაგერმა 1962 წელს. ისინი გარკვეული დროით მივიწყებულ იქნა ამ დრომდე, სანამ ხელმეორედ არ აღმოაჩინეს და წამოაყენეს ახალი ინტერესები.

LDPC კოდი არის შეცდომის - გასწორების კოდი, რომელიც განისაზღვრება r ×l პარიტეტული - შემოწმების მატრიცის $H \in GF(2)^{rl}$ კონკრეტული ფორმით. უფრო კონკრეტულად რომ ვთქვათ, LDPC კოდების ოჯახი ხასიათდება არა - ნულოვანი ჩანაწერების პროპორციით თითოეულ მწკრივსა და სვეტში, რომელიც დაჯამებულია ორი ფორმალური მრავალწევრის მიერ

$$L(x) = \sum_k L_k x^k \text{ and } R(x) = \sum_k R_k x^k \qquad (54)$$

მრავალწევრი L(x) (ან R(x)) აღნიშნავს არა - ნულოვანი ჩანაწერების პროპორციას H სვეტებში (ან მწკრივებში), ე.ი.,

$L_k = l^{-1}|\{j : \text{სვეტი } HF\cdot j \text{ შეიცავს } k\}|$,

$R_k = r^{-1}|\{i : \text{მწკრივი } HF_i\cdot \text{ შეიცავს } k\}|$.

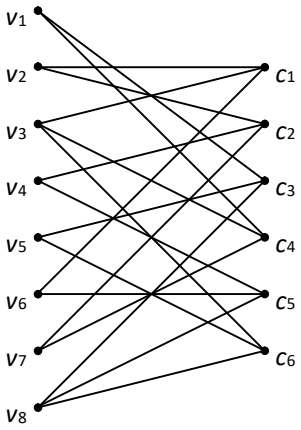
L(x) და R(x) მრავალწევრიანი LDPC კოდისთვის, პარიტეტული შემოწმების მატრიცა შესაბამისად შეიცავს $E(l) = l\sum_k kL_k = r\sum_k kR_k$ არა - ნულოვანი ჩანაწერების ჯამს. ეს რიცხვი E(l) იზრდება მხოლოდ ბლოკის სიდიდის HP l პროპორციულად, მაშინ როცა შემთხვევითად - შერჩეული მატრიცა HF შეიცავს არა - ნულოვანი ჩანაწერების კვადრატულ რიცხვს (ე.ი. იმის

გათვალისწინებით, რომ r პროპორციულია l -ის). ეს არის LDPC კოდების მსაზღვრელის დაბალი სიხშირის მიზეზი.

განსაზღვრული მატრიცის სიდიდის მქონე ყველა LDPC კოდს, რომელსაც ახასიათებს იგივე მრავალწევრები L(x) და R(x), აქვს თითქმის იგივე თვისებები. აქედან გამომდინარე, ჩვენი მიზნებისთვის საკმარისია LDPC კოდი მივიჩნიოთ ნაკრებიდან შემთხვევითად შერჩეულად; დიდი ალბათობით, ასეთი კოდი ისეთივე კარგი იქნება როგორც ნაკრების ნებისმიერი სხვა კოდი.

ვინაიდან გვსურს LDPC კოდების გამოყენება შესათანხმებლად, ყურადღებას ვამახვილებთ მეორეხარისხოვანი მონაცემებით საწყისი კოდირების პრობლემაზე. დასაშიფრად ელისი უგზავნის ბობს მისი გასაღების ელემენტების სინდრომს, ე.ი. ის უგზავნის Ξ = HFX. გაითვალისწინეთ, რომ ეს ოპერაცია მოითხოვს მხოლოდ E(l) ორობით ოპერაციებს, რომელიც ბლოკის სიდიდის l პროპორციულია.

გაშიფვრისთვის ბობი იყენებს LLR -ზე დაფუძნებულ განმეორებად პროცესს, ტურბო კოდების მსგავსი მეთოდით. სანამ დაწვრილებით ავღწერთ გაშიფვრის პროცესს, უკეთესია დავახასიათოთ LDPC კოდები ტანერის გრაფების სახით. მოცემული LDPC კოდისთვის, დავუშვათ მასთან დაკავშირებულ ტანერის გრაფას G(H) აქვს l + r წვერები $v_{1\ldots l}$ და $c_{1\ldots r}$ -ის ერთობლიობა, სახელწოდებით ცვლადების კვანძები და შემოწმების კვანძები, შესაბამისად. ტანერის გრაფის კიდეები განისაზღვრება მატრიცით H: კიდე აკავშირებს v_j -ას c_i -თან თუ $HF_{ij} = 1$. აქედან გამომდინარე, ტანერის გრაფა არის ორმხრივი გრაფა E(l) კიდეებით.



ნახაზი 18. მრვალწევრების მქონე ზოგიერთი თვითნებური 6 × 8 LDPC კოდის ტანერის გრაფა

$$L(x) = \frac{6}{8}x^2 + \frac{2}{8}x^3 \text{ and } R(x) = \frac{6}{6}x^3 \ .$$

გრაფიკის თვალსაზრისით, L(x) და R(x) მრავალწევრები იძლევა ცვლადი კვანძების და შემოწმების კვანძების ხარისხებს, შესაბამისად. კერძოდ, L_k ცვლადი კვანძები არის k ხარისხის, ხოლო rR_k შემოწმების კვანძები არის k ხარისხის.

გაშიფვრის (დეკოდირების) პროცესი შეიძლება დახასიათდეს, როგორც შეტყობინებების გაცვლა ცვლად და შემოწმების კვანძებს შორის. კერძოდ, მოდით ამჯერად ავღწეროთ შეტყობინების გადაცემის (belief propagation) გაშიფვრის ალგორითმი. ბობი იყენებს პროცედურას მომდევნო რიგის გაყოლებით. პირველი, ცვლადი კვანძები აგზავნის ხმაურიან სიდიდეებს y მოსაზღვრე შემოწმების კვანძების მიმართ. შემოწმების კვანძებმა უნდა მიიღონ სიდიდეები ცვლადი კვანძებიდან, რომელთა ჯამია ξ. ამ მტკიცებულების საფუძველზე, შემოწმების კვანძები შემდეგ უკან უგზავნიან ცვლად კვანძებს იმას რასაც x -ის სწორ სიდიდედ „მიიჩნევენ“. ვინაიდან y არის ხმაურიანი, იგი შეიძლება პირველად გაგზავნილი სიდიდეების ტოლი იყოს ან განსხვავდებოდეს მათგან. ამჯერად, ცვლადი კვანძები იღებენ სხვადასხვა შემოწმების კვანძების დასკვნას, რაც აძლევს მათ x -ის უფრო ზუსტ სიდიდეს (ე.ი., X -ის LLR). ეს ახალი სიდიდე კვლავ გადაეცემა შემოწმების კვანძებს, და ასე შემდეგ.

პროცედურის ზუსტი ფორმის აღსაწერად მოვიშველიოთ მარტივი მაგალითი. ჩავთვალოთ, რომ ბობმა უკვე იცის ალისას მიერ გაგზავნილი x სწორი სიდიდე. როგორც შეტყობინების გადაცემის ალგორითმის ნაწილი, თითოეული ცვლადი კვანძი v_j შეტყობინების სახით პირველად აგზავნის შესაბამისი ბიტის x_j სიდიდეს მოსაზღვრე შემოწმების კვანძის მისამართით hc_i (ე.ი., $HF_{ij} = 1$ -ის შემთხვევისთვის, ისე რომ არსებობდეს კიდე v_j და hc_i -ის შორის). hc_i კვანძის თვალსაზრისით, ყველა მიღებული შეტყობინება უნდა დაჯამდეს ξ_i -მდე, ვინაიდან $\xi_i = \sum_j HF_{ij}x_j$. შემდეგ, შემოწმების კვანძი hc_i ცვლადი კვანძის v_j მიმართულებით აგზავნის

$\xi_i + \sum_{j' \neq j} HF_{ij'}x_{j'}$ მნიშვნელობას. ცვლადი კვანძის vPj პერსპექტივიდან გამომდინარე, მან უნდა მიიღოს x_j მნიშვნელობა ყველა მოსაზღვრე შემოწმების კვანძიდან, ვინაიდან $\xi_i + \sum_{j' \neq j} HF_{ij'}x_{j'} = x_j$

რა თქმა უნდა, ბობს წვდომა აქვს მხოლოდ პარიტეტულ ბიტებზე ξ და საკუთარი გასაღების ელემენტებზე y, რომელიც წარმოადგენს გასაღების ელემენტების x ხმაურიან ვარიანტს, რომლის აღდგენაც მას სურს. შეტყობინების გადაცემის ალგორითმი განმარტავს ზემოთ მოყვანილ მარტივ მაგალითს LLR -ის გათვალისწინებით. პირველი ეტაპისთვის, ცვლადი კვანძი vj იცნობს მხოლოდ yj -ის. ბობი აფასებს შესაბამის LLR -ს

$$L_{v_j \to hc} = L(X_j \mid y_j) = \ln \frac{H\Pr[X_j=0, Y_j=y_j]}{HPr[X_j=1, Y_j=y_j]},$$

რომელიც გადაეცემა შემოწმების კვანძებს. შემდეგ, $\xi_i + \sum_{j' \neq j} HF_{ij'}x_{j'}$ ფორმულირების LLR უკანვე უნდა გადაეცეს ცვლად კვანძს v_j. იმისათვის რომ დავინახოთ, თუ როგორ მუშაობს იგი, მოდით შევაფასოთ ორი ბიტის $X_1 + X_2$ ჯამის LLR:

$$\begin{aligned}\mathrm{HL}(\mathrm{X}_1+\mathrm{X}_2 \mid \mathrm{y}_1,\mathrm{y}_2) &= \ln\frac{\mathrm{HP}_{\mathrm{X}_1+\mathrm{X}_2,\mathrm{Y}_1,\mathrm{Y}_2}(0,\mathrm{y}_1,\mathrm{y}_2)}{\mathrm{HP}_{\mathrm{X}_1+\mathrm{X}_2,\mathrm{Y}_1,\mathrm{Y}_2}(1,\mathrm{y}_1,\mathrm{y}_2)}\\ &= \ln\frac{\mathrm{HP}_{\mathrm{X}_1\mathrm{Y}_1}(0,\mathrm{y}_1)H\mathrm{P}_{\mathrm{X}_2\mathrm{Y}_2}(0,\mathrm{y}_2)+\mathrm{HP}_{\mathrm{X}_1\mathrm{Y}_1}(1,\mathrm{y}_1)\mathrm{HP}_{\mathrm{X}_2\mathrm{Y}_2}(1,\mathrm{y}_2)}{\mathrm{HP}_{\mathrm{X}_1\mathrm{Y}_1}(0,\mathrm{y}_1)\mathrm{HP}_{\mathrm{X}_2\mathrm{Y}_2}(1,\mathrm{y}_2)+\mathrm{HP}_{\mathrm{X}_1\mathrm{Y}_1}(1,\mathrm{y}_1)H\mathrm{P}_{\mathrm{X}_2\mathrm{Y}_2}(0,\mathrm{y}_2)}\\ &= \frac{\frac{H\mathrm{P}_{\mathrm{X}_1\mathrm{Y}_1}(0,\mathrm{y}_1)}{\mathrm{HP}_{\mathrm{X}_1\mathrm{Y}_1}(1,\mathrm{y}_1)}\times\frac{\mathrm{HP}_{\mathrm{X}_2}\mathrm{Y}_2(0,\mathrm{y}_2)}{H\mathrm{P}_{\mathrm{X}_2\mathrm{Y}_2}(1,\mathrm{y}_2)}+1}{\frac{\mathrm{HP}_{\mathrm{X}_1\mathrm{Y}_1}(0,\mathrm{y}_1)}{H\mathrm{P}_{\mathrm{X}_1\mathrm{Y}_1}(1,\mathrm{y}_1)}+\frac{H\mathrm{P}_{\mathrm{X}_2\mathrm{Y}_2}(0,\mathrm{y}_2)}{\mathrm{HP}_{\mathrm{X}_2\mathrm{Y}_2}(1,\mathrm{y}_2)}}\\ &= \ln\frac{\mathrm{e}^{\mathrm{HL}_1}\mathrm{e}^{\mathrm{HL}_2}+1}{\mathrm{e}^{\mathrm{HL}_1}+\mathrm{e}^{H\mathrm{L}_2}} = \ln\frac{\frac{\mathrm{e}^{\mathrm{HL}_1}+1}{\mathrm{e}^{\mathrm{hL}_1-1}}\frac{\mathrm{e}^{\mathrm{HL}_2}+1}{\mathrm{e}^{\mathrm{HL}_2-1}}+1}{\mathrm{e}^{\mathrm{HL}_1+1}\mathrm{e}^{\mathrm{HL}_2+1}-1}\mathrm{e}^{\mathrm{HL}_2-1}-1\\ &= \phi^{-1}\big(\phi(H\mathrm{L}_1)\phi(\mathrm{HL}_2)\big),\end{aligned}$$

with $\mathrm{HL_i} = \mathrm{HL}(\mathrm{X_i} \mid \mathrm{y_i})$ and

$$\phi(\mathrm{HL}) = \frac{\mathrm{e}^{\mathrm{HL}}+1}{\mathrm{e}^{\mathrm{HL}}-1}, \phi^{-1}(\lambda) = \ln\frac{\lambda+1}{\lambda-1}.$$

რამოდენიმე ბიტის ჯამის გენერალიზება პირდაპირ ხდება. აქედან გამომდინარე, $\xi_i + \sum_{j'\neq j} HF_{ij'}x_{j'}$ გამოსახულების LLR შემდეგნაირად ჩამოყალიბდება

$$HL_{c_i\to v_j} = (-1)^{\xi_i}\phi^{-1}\left(\prod_{j'\neq j:HF_{ij'}=1}\phi\left(L_{v_{j'}\to c}\right)\right).$$

გაითვალისწინეთ, რომ $(-1)^{\xi i}$ მამრავლი გამომდინარეობს იმ ფაქტიდან, რომ ξ დარწმუნებით ცნობილია და რომ $\varphi^{-1}(\varphi(\pm\infty)\varphi(\mathrm{HL})) = \pm\mathrm{L}$.

ცვლადი კვანძები LLR -ს იღებენ ყველა მომიჯნავე შემოწმების კვანძებიდან. როგორ შეძლებს ბობი X -ის LLR -ის შეფასების დამუშავებას ამ მონაცემების გამოყენებით? ამისათვის, შეტყობინების გადაცემის ალგორითმი ამუშავებს შემოსულ LLR -ს ისე თითქოს იგი დამოუკიდებელი დაკვირვების შედეგიდან გამომდინარეობდეს. დავუშვათ, რომ ზოგიერთ ცვლადი X' განისაზღვრება $Y_{1\ldots n}$ ცვლადებით, ისე რომ

$$\mathrm{HPr}\left[Y_{1\ldots n} = y_{1\ldots n} \mid X' = x'\right] = \prod_i \mathrm{HPr}\left[Y_i = y_i \mid X' = x'\right]$$

მაშინ,

$$\mathrm{L}(\mathrm{X}' \mid \mathrm{y}_{1\ldots\mathrm{n}}) = \ln \frac{\mathrm{HPr}[\mathrm{Y}_{1\ldots\mathrm{n}} = \mathrm{y}_{1\ldots\mathrm{n}} \mid \mathrm{X}' = 0]}{\mathrm{HPr}[\mathrm{Y}_{1\ldots\mathrm{n}} = \mathrm{y}_{1\ldots\mathrm{n}} \mid \mathrm{X}' = 1]}$$
$$= \ln \frac{\prod_{\mathrm{i}} \mathrm{HPr}\,[\mathrm{Y}_{\mathrm{i}} = \mathrm{y}_{\mathrm{i}} \mid \mathrm{X}' = 0]}{\prod_{\mathrm{i}} \mathrm{HPr}\,[\mathrm{Y}_{\mathrm{i}} = \mathrm{y}_{\mathrm{i}} \mid \mathrm{X}' = 1]} = \sum_{\mathrm{i}} \mathrm{L}(\mathrm{X}' \mid \mathrm{y}_{\mathrm{i}})$$

ამრიგად, დამოუკიდებელი დაკვირვების შედეგის თეორიის თანახმად, LLR -ის შეჯამება შესაძლებელია. x_j -ის შემთხვევაში, ცვლადი კვანძი v_j ითვალისწინებს ორივეს, LLR $L(X_j|y_j)$ და LLR, რომელსაც იძლევა მომიჯნავე შემოწმების კვანძები $L_{ci}\rightarrow v_j$. აქედან გამომდინარე, LLR -ის გადაცემის წესი ცვლად კვანძზე ჩამოყალიბდება შემდეგნაირად

$HL_{v_j \to c} = HL(X_j \mid y_j) + \sum HL_{c_i \to v_j}$.

ეს პროცესი მეორდება სანამ არ მიიღწევა კონვერგენცია ან გამეორებების ფიქსირებული რიცხვი.

თავი 8. ახალი სქემა

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. ბენეტის და ბრასარდის მიერ BB84 პროტოკოლის გამოშვება 1984 წელს აღნიშნავს გასაღების კვანტური განაწილების დასაწყისს. მას შემდეგ, მრავალ სხვა პროტოკოლებს იგონებენ. თუმცა, BB84 -ს პრივილეგირებული ადგილი უკავია არსებულ პროტოკოლთა სიაში: ეს ის არის, რომელსაც ყველაზე მეტად აანალიზებენ და ყველაზე ხშირად ანხორციელებენ, მათ შორის მათ, რომელიც კომერციულ პროდუქტებში გამოიყენება. განვმარტავთ BB84 პროტოკოლს, მიუხედავად იმისა, რომ არაფორმარულად უკვე ავღწერეთ. ამის შემდგომ შესწავლილია ფიზიკური განხორციელება. დაბოლოს, ვაანალიზებთ მოსმენის (მიყურადების) სტრატეგიებს BB84 -ის მიმართ და დავადგენთ საიდუმლო გასაღების მაჩვენებელს.

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

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

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.

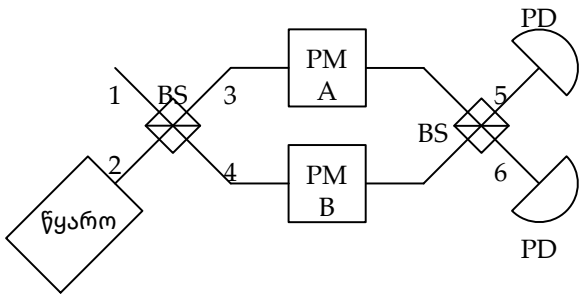
პირველი, BB84 -ის მიერ დადგენილი ინფორმაციის მატარებლები იდეალურად წარმოადგენს ერთ ფოტონიან მდგომარეობებს. თუმცა, რთულია მათი წარმოება, და ალტერნატიული გამოსავალი არის სუსტი თანმიმდევრული მდგომარეობების გამოყენება, ანუ, თანმიმდევრული მდგომარეობები ფოტონების დაბალი საშუალო რიცხვით, რათა მიუახლოვდეს ერთ - 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.

დაბოლოს, 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.

8.1 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.



ნახაზი 19. ფაზური დაშიფვრა

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). მაჩ - ზენდერის ინტერფერომეტრი

მოდით განვიხილოთ 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 n_1 -ში და ერთადერთი ფოტონია n_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 n_4 -ში არსებული ფოტონისთვის. შემდეგ, ფაზათა გადანაცვლება ხდება ორ მხარში. მნიშვნელოვანია მხოლოდ ფარდობითი ფაზა $\varphi = \varphi_{\mathrm{A}} - \varphi_{\mathrm{B}}$, 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. n_3 -ში არსებული ფოტონი გარდაიქმნება ამგვარად $|01\rangle_{\mathrm{nm_3 n_4}} \rightarrow \left(i|10\rangle_{\mathrm{nm_5 nm_6}} + |01\rangle_{\mathrm{nm_5 nm_6}}\right)/\sqrt{2}$, ხოლო ფოტონი n_4 გარდაიქმნება ასეთი სახით $|01\rangle_{\mathrm{nm_3 nm_4}} \rightarrow \left(|10\rangle_{\mathrm{nm_5 nm_6}} + \mathrm{i}|01\rangle_{\mathrm{nm_5 nm_6}}\right)/\sqrt{2}$. ფაზათა გადანაცვლებიდან გამომდინარე $\varphi = 0, \pi/2, \pi$ or $3\pi/4$, ალგებრა უზრუნველყოფს შემდეგ გამომავალ მდგომარეობებს:

$$\begin{aligned}
|\psi(\phi = 0)\rangle &= \mathrm{i}|01\rangle_{\mathrm{nm_5 nm_6}} \\
|\psi(\phi = \pi/2)\rangle &= \left(\mathrm{i}|01\rangle_{\mathrm{nm_5 nm_6}} + \mathrm{i}|10\rangle_{\mathrm{nm_5 nm_6}}\right)/\sqrt{2}, \\
|\psi(\phi = \pi)\rangle &= \mathrm{i}|10\rangle_{\mathrm{nm_5 nm_6}} \\
|\psi(\phi = 3\pi/2)\rangle &= \left(\mathrm{i}|01\rangle_{\mathrm{nm_5 nm_6}} - \mathrm{i}|10\rangle_{\mathrm{nm_5 nm_6}}\right)/\sqrt{2}.
\end{aligned}$$

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

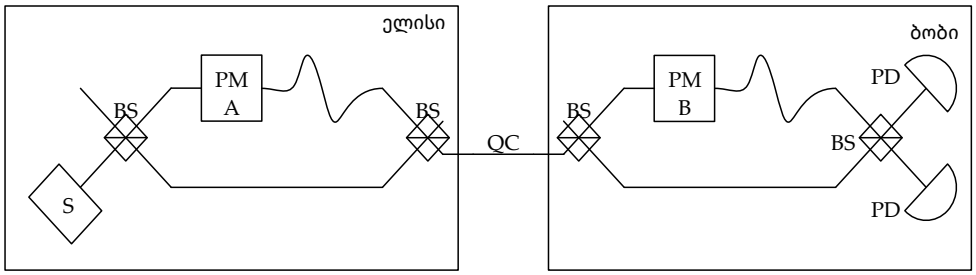
$$|\psi(\phi = 0)\rangle = |0\rangle$$
$$\left|\psi\left(\phi = \frac{\pi}{2}\right)\right\rangle = |+\rangle$$
$$|\psi(\phi = \pi)\rangle = |1\rangle$$
$$\left|\psi\left(\phi = 3\frac{\pi}{2}\right)\right\rangle = |-\rangle$$

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, სირთულეს წარმოადგენს, რადგან ბოჭკოვანი ოპტიკის ორი მხარის სიგრძე ზუსტად უნდა ემთხვეოდეს ტალღის სიგრძის ნაწილს. ალისას და ბობს შორის დავუშვათ ათობით კილომეტრი, ტემპერატურის ნებისმიერი ცვლილება გააფართოვებს ან შეამცირებს ბოჭკოს, სიდიდის უმნიშვნელო ხარისხით, რომელიც ტალღის სიგრძეზე გრძელია.

ამის თავიდან ასაცილებლად უნდა გამოვიყენოთ მაჩ - ზენდერის კონსტრუქცია, რომელიც ნახაზი 20-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 20. 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).

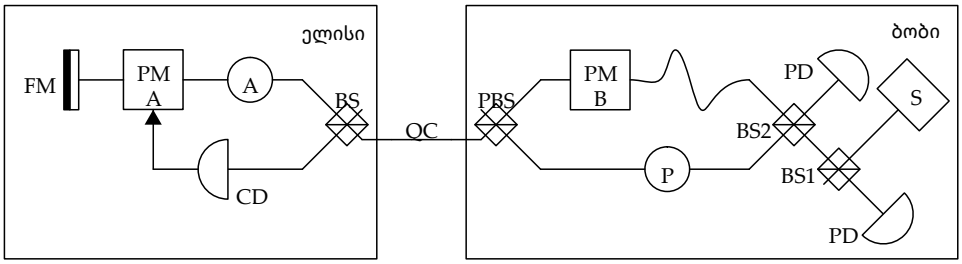
მიღების მომენტი განსხვავებული იქნება და შესაბამისად, ამ შემთხვევების გარჩევა შეიძლება. გაითვალისწინეთ რომ მიღების მომენტი იგივე იქნება ფოტონისთვის, რომელიც გაედინება ჯერ გრძელ მხარში და შემდეგ მოკლე მხარში ან პირიქით. აქედან გამომდინარე, თუ ჩვენ მხოლოდ შუა მიღების მომენტს შევხედავთ, ორი „ნახევარი“ ფოტონი განიცდის ინტერფერენციას, ერთი გადის ალისას 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.

8.2 Plug – and – play (დანამატი და თამაში) კონსტრუქცია

შემდგომი კონსტრუქცია, სახელწოდებით დანამატი - და - თამაში (plug-and-play), იძლევა ავტომატური ოპტიკური განლაგების საშუალებას და ილუსტრირებულია ნახაზზე 21. იდეა იმაში მდგომარეობს, რომ გააერთიანოს მაჩ - ზენდერის კონსტრუქცია დროის მალტიპლექსირების და ორთოგონალურ პოლარიზაციასთან. მოდით უფრო დეტალურად ავღწეროთ ეს კონსტრუქცია.

ამ კონსტრუქციაში იმპულსები ინიცირებულია ბობის და არა ალისას მიერ. მიუხედავად ამისა, ბობის მიერ გაგზავნილი იმპულსები ყოველთვის იდენტურია და არ შეიცავს რაიმე ინფორმაციას. ბობი ქმნის (კლასიკურ) ძლიერ იმპულსს, რომელიც იყოფა ორ იმპულსად სხივ გამყოფის მიერ BS2. ინტენსივობის ნახევარი მიდის მოკლე მხარში (იმპულსი p_1), ხოლო მეორე

ნახევარი მიდის გრძელ მხარში (იმპულსი p_2). ამ ეტაპზე, ბობის ფაზური მოდულატორი უმოქმედოა, ასე რომ გრძელი მხარი არაფერს არ აკეთებს იმპულსის შეფერხების გარდა. p_2 -ის პოლარიზაცია ირჩევა ისე, რომ იგი გადაიცემა პოლარიზებული სხივ გამყოფის მიერ კვანტურ არხში. თუმცა, მოკლე მხარში იმპულსის p_1 პოლარიზაციის როტაცია ხდება 90^0 -ით, ასე რომ მას აირეკლავს პოლარიზებული სხივ გამყოფი და შეჰყავს კვანტურ არხში.



ნახაზი 21. „დანამატი და თამაშის“ (Plug-and-play) კონსტრუქცია.

ბობის სადგური შედგება წყაროსგან (S), რომელიც შედის ბოჭკოში სხივ გამყოფის (BS1) საშუალებით. ბობის სადგურის ორი მხარი ერთმანეთთან დაკავშირებულია სხივ გამყოფით (BS2) და პოლარიზებული სხივ გამყოფით (PBS). გრძელი მხარი შეიცავს ფაზურ მოდულატორს (PMB), რომელიც აქტიურია მხოლოდ მაშინ, როცა იმპულსები ბრუნდება ბობის სადგურში. მოკლე მხარი შეიცავს პოლარიზატორს (P), რომელიც ახდენს პოლარიზაციის როტაციას 90^0 -ით. იმპულსები გაედინება კვანტურ არხში (QC). ელისის სადგური მოიცავს სხივ გამყოფს (BS). ზედა მხარზე, იმპულსები წარიმართება ატენუატორის (A) და ფაზური მოდულატორის (PMA) მეშვეობით, რომელიც აქტიურია მხოლოდ მეორე იმპულსისთვის. ფარადეის სარკე (FM) ირეკლავს იმპულსებს და ახდენს მათი პოლარიზაციის როტაციას 90^0 -ით. ქვედა მხარზე, იმპულსები ვლინდება კლასიკური დეტექტორით (CD).

ბობის სადგურის გამოსასვლელში, ორი იმპულსი გადაიცემა ოდნავ განსხვავებულ დროებში (პირველი p_1, შემდეგ p_2) და ორთოგონალური პოლარიზაციით.

როდესაც პირველი იმპულსი (p_1) შედის ალისას სადგურში, ინტენსივობის ნახევარი შედის ზედა მხარში. ამ ეტაპზე, ასევე უმოქმედოა ალისას ფაზური მოდულატორი. იმპულსი სუსტდება ატენუატორის საშუალებით და აირეკლება ფარადეის სარკით, რომელიც ახდენს მისი პოლარიზაციის როტაციას 90^0 -ით.

p_1 -ის ნახევარი ასევე შედის ქვედა მხარში და დეტექტორში. დეტექტორს მოქმედებაში მოყავს ალისას ფაზური მოდულატორი, რომელიც ახლა უკვე მზადაა მეორე იმპულსისთვის. როდესაც მეორე იმპულსი p_2 შედის ალისას სადგურში, ინტენსივობის ნახევარი შედის ზედა მხარში. რაც შეეხება პირველ იმპულსს, მეორე იმპულსი სუსტდება და მისი პოლარიზაციის როტაცია ხდება 90^0 -ით. რადგან ალისას ფაზური მოდულატორი ახლა უკვე აქტიურია, p_2 -ის ფაზა მოდულირდება φ_A -ით.

იმპულსები ამჯერად უბრუნდება ბობს. ალისას სადგურის შესასვლელში, ორი იმპულსი ძლიერ შესუსტდა და აქვს კვანტური ხასიათი. ისინი კვლავ გამოყოფილია იმავე შეფერხების გამო და ისევ აქვს ორთოგონალური პოლარიზაცია; თუმცა, მეორე იმპულსი p_2 ფაზით - მოდულირებულია და შიფრავს ალისას საიდუმლო გასაღების ბიტს.

ბობის სადგურში შესვლისას, p_1 გადაიცემა პოლარიზაციის სხივ გამყოფით. ეს გამოწვეულია ფარადეის სარკით, რომელმაც მოახდინა იმპულსების როტაცია. იმპულსი p_1 ამჯერად გადის გრძელ მხარში და ფაზით - მოდულირდება φ_B -ის მიერ. ანალოგიურად, მეორე იმპულსი p_2 აირეკლება პოლარიზაციის სხივ გამყოფით და გადის მოკლე მხარში. იმის გამო, რომ მათ გაიარეს იგივე მანძილი, ორი იმპულსი ერთდროულად ხვდება სხივ გამყოფთან და ურთიერთქმედებენ როგორც რეგულარულ მაჩ - ზენდერის ინტერფერომეტრში.

ამ კონსტრუქციას აქვს უპირატესობა უზრუნველყოს თვით- კომპენსაცია ვარიაციებისთვის წრედის სიგრძეში და ბოჭკოთი გამოწვეული პოლარიზაციის ცვლილებისთვის. პირველი, გზის ორივე მანძილი ზუსტად იგივეა ორი იმპულსისთვის. ისინი ორივე გადიან ბობის სადგურის მოკლე

და გრძელ მხრებს, მაგრამ სხვადასხვა დროს. მეორე, ფარადეის სარკის გამოყენება აუქმებს პოლარიზაციის ცვლილებებს ბოჭკოზე. რომ არ ჩავუღრმავდეთ დეტალებს, პოლარიზაციის ყველა ცვლილება, მათ შორის ორმაგი სხივთტეხა, კომპენსირდება დასაბრუნებელი მარშრუტის განმავლობაში, როცა იმპულსები მიედინებიან ბობიდან ალისასკენ. იმპულსის პოლარიზაცია, როცა ბრუნდება ბობის პოლარიზაციის სხივ გამყოფს, ზუსტად იმ პოლარიზაციის ორთოგონალურია, რომელიც მას ჰქონდა, როცა ტოვებდა ბობის სადგურს.

ეს ნაწილი აჯამებს ფაზური დაშიფვრის მეთოდების მიმოხილვას.

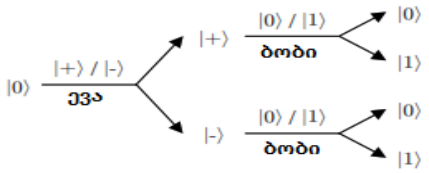
ექსპერიმენტული იმპლემენტაციები ფაზური დაშიფვრის საშუალებით, მრავალია. არსებობს „დანამატი და თამაში“ (plug-and-play), რომელიც განხორციელდა ზბინდენის, რიბორდის, სტუკის მიერ, რომელიც გამოიყენებოდა ჟენევასა და ნიონს შორის გასაღების გასანაწილებლად შვეიცარიაში, ტბა ჟენევას ქვეშ და 67კმ-ზე მეტ მანძილზე ჟენევასა და ლოზანას შორის, შვეიცარია. ფაზურ დაშიფვრაზე დაფუძნებულ სხვა სისტემებს გვთავაზობს ბეთუნი, ნავარო და რისკი და ბურენანი. დაბოლოს, გობიმ, იუანმა და შილდსმა აჩვენეს სამუშაო სისტემა, რომლის დიაპაზონი 122 კმ -მდე იყო.

მოსმენის ამოცნობა: 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⟩ ან |1⟩). ყველა შემთხვევაში, როდესაც ევა იჭერს ფოტონს, ის ზომავს მას და უგზავნის ბობს, მას აქვს ¼ შეცდომის ალბათობა ალისას და ბობის ბიტებს შორის.

მოდით ვუარყოთ 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.|+⟩ან|−⟩,|0⟩ან|1⟩ ნაცვლად ამისა). სიტუაცია აღწერილი არასწორი პოზიციისას, ბობი ძირითადად ზომავს შემთხვევით ბიტს, რომელსაც გააჩნია ალისას ბიტთან დამთხვევის ½ ალბათობა და შეცდომის ½ ალბათობა.



ნახაზი 22. 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 რომელიც 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 n ინდექსს (მაგ.n = 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 I_E ან უბრალოდ რამოდენიმე წარმოებული ფუნქციის l შედეგი, რომელიც იძლევა I_E 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, სახელწორდებით 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 $\mathrm{f}(x_1 + x_2)mod\,2$, 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 x_1აქვს. ფასი, რომლის გადახდაც 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 $|Mes|$. დაბოლოს, კონფიდენციალურობის გაძლიერების შემდეგ მიღებული საიდუმლო გასაღები, შეიძლება გამოყენებულ იქნას ელისისა და ბობის მიერ კრიფტოგრაფიული მიზნებისთვის. კერძოდ, მათ შეუძლიათ გამოიყენონ გასაღები შეტყობინების დასაშიფრად ან საიდუმლო არხის შესაქმნელად.

შეტყობინების ხელმოსაწერად გენერირდება ხელმოწერის და ვერიფიკაციის გასაღებები. ამისათვის, ვინტერნიცის პარამეტრი არის hw >= 2, და იგი არის ბიტების რაოდენობის ტოლი, რომლის ხელმოწერად ერთდროულად უნდა მოხდეს. გამოთვლილ უნდა იქნას $v_1=n/hw$ და $v_2=(\log_2 v_1 +1+hw)/hw$, $v= v_1+ v_2$ - თან ერთად. ხელმოწერის გასაღები *X* შეიცავს *v* სიგრძის *2n* შემთხვევით მწკრივებს. მისი ვერიფიკაციის გასაღები *Y* იგივე სიდიდისაა.

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

$Y= (y_{v-1}[0], y_{v-1}[1], y_{v-2}[0], y_{v-2}[1], \ldots, y_0[0], y_0[1]) \in \{0,1\}^{v,2n}$, სადაც $y_i=f_o^{2\wedge hw-1}(x_i)$, 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: $hashf=k_{p-1},\ldots, k_{p-p1}$. საკონტროლო ჯამი გამოითვლება შემდეგნაირად:$hc=\sum_{i=v-v1}^{v-1}(2^{hw}-hp_i)$. იმის გათვალისწინებით, რომ $c<= v_1 2^{hw}$, ორობითი გამოსახულების სიგრძე არის $\log_2 v_1 2^w+1$. ნულების მინიმალური რაოდენობა ემატება ორობით გამოსახულებას, რათა მივიღოთ გამოსახულების სიგრძე, რომელიც იყოფა *w*-ზე. შედეგად, იგი იყოფა *w* სიგრძის *v2* ნაწილებად. შეტყობინებაზე ხელმოწერა ხდება შემდეგნაირად: $SIG=(f_o\wedge p_{v-1}(x_{v-1}), \ldots, f_o\wedge p_0(x_0))$.

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

დასკვნა.

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 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.

პოსტ კვანტურში დაგვრჩა ხელმოწერის ეფექტურობის გაუმჯობესების საკითხი.

შესწავლილი იქნა ჰეშზე დაფუძნებული ხელმოწერის სქემები, რომლებიც, ხაზგასმით უნდა აღინიშნოს, რომ მდგრადები არიან პოსტ კვანტურ ეპოქაში და შერჩეულ 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.

მიღებული შედეგიდან გამომდინარე აღსანიშნავია, რომ ვიყენებთ ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემას, რომელიც 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 შემთხვევაში.

ლიტერატურის ნუსხა.

1. Boneh D. and Shoup V., A Graduate Course in Applied Cryptography, http://toc.cryptobook.us/, 2020
2. Mollin, R.A. An Introduction to Cryptography (2nd ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781420011241, 2006
3. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, Chapman and Hall/CRC, 2020
4. Deavours: Cipher A. Deavours and Louis Kruh, ``Machine Cryptography and Modern Cryptanalysis'', Artech House, 1985
5. Schneier B., Applied Cryptography, 2nd ed., John Wiley & Sons, 1996
6. Shor P. W., "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.
7. Toyama, F.M., van Dijk, W. & Nogami, Y. Quantum search with certainty based on modified Grover algorithms: optimum choice of parameters. Quantum Inf Process 12, 1897–1914 (2013). https://doi.org/10.1007/s11128-012-0498-0

8. Z. Qu, Z. Li, G. Xu, S. Wu and X. Wang, "Quantum Image Steganography Protocol Based on Quantum Image Expansion and Grover Search Algorithm," in IEEE Access, vol. 7, pp. 50849-50857, 2019, doi: 10.1109/ACCESS.2019.2909906.
9. Jaques S., Naehrig M., Roetteler M., Virdia F. (2020) Implementing Grover Oracles for Quantum Key Search on AES and LowMC. In: Canteaut A., Ishai Y. (eds) Advances in Cryptology – EUROCRYPT 2020. EUROCRYPT 2020. Lecture Notes in Computer Science, vol 12106. Springer, Cham. https://doi.org/10.1007/978-3-030-45724-2_10
10. Biswas B., Sendrier N. (2008) McEliece Cryptosystem Implementation: Theory and Practice. In: Buchmann J., Ding J. (eds) Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science, vol 5299. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88403-3_4
11. Canteaut A., Sendrier N. (2000) Cryptanalysis of the Original McEliece Cryptosystem. In: Ohta K., Pei D. (eds) Advances in Cryptology — ASIACRYPT'98. ASIACRYPT 1998. Lecture Notes in Computer Science, vol 1514. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-49649-1_16
12. Loidreau P. (2000) Strengthening McEliece Cryptosystem. In: Okamoto T. (eds) Advances in Cryptology — ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science, vol 1976. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44448-3_45

13. 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

14. Bernstein D.J. (2009) Introduction to post-quantum cryptography. 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_1
15. Bernstein D.J. et al. (2015) SPHINCS: Practical Stateless Hash-Based Signatures. In: Oswald E., Fischlin M. (eds) Advances in Cryptology -- EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol 9056. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-46800-5_15
16. McGrew D., Kampanakis P., Fluhrer S., Gazdag SL., Butin D., Buchmann J. (2016) State Management for Hash-Based Signatures. In: Chen L., McGrew D., Mitchell C. (eds) Security Standardisation Research. SSR 2016. Lecture Notes in Computer Science, vol 10074. Springer, Cham. https://doi.org/10.1007/978-3-319-49100-4_11
17. Bernstein D.J., Chou T., Schwabe P. (2013) McBits: Fast Constant-Time Code-Based Cryptography. In: Bertoni G., Coron JS. (eds) Cryptographic Hardware and Embedded Systems - CHES 2013. CHES 2013. Lecture Notes in Computer Science, vol 8086. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40349-1_15
18. N. Sendrier, "Code-Based Cryptography: State of the Art and Perspectives," in IEEE Security & Privacy, vol. 15, no. 4, pp. 44-50, 2017, doi: 10.1109/MSP.2017.3151345.
19. Chou T. (2016) QcBits: Constant-Time Small-Key Code-Based Cryptography. In: Gierlichs B., Poschmann A. (eds) Cryptographic Hardware and Embedded Systems – CHES 2016. CHES 2016. Lecture Notes in Computer Science, vol 9813. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-53140-2_14
20. Buchmann J., Lauter K. and Mosca M., "Postquantum Cryptography—State of the Art," in IEEE Security & Privacy, vol. 15, no. 4, pp. 12-13, 2017, doi: 10.1109/MSP.2017.3151326.
21. Lauter K., "The advantages of elliptic curve cryptography for wireless security," in IEEE Wireless Communications, vol. 11, no. 1, pp. 62-67, Feb. 2004, doi: 10.1109/MWC.2004.1269719.
22. Hankerson D., López Hernandez J., Menezes A. (2000) Software Implementation of Elliptic Curve Cryptography over Binary Fields. In: Koç Ç.K., Paar C. (eds) Cryptographic Hardware and Embedded Systems —

CHES 2000. CHES 2000. Lecture Notes in Computer Science, vol 1965. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44499-8_1
23. Neve M., Seifert JP. (2007) Advances on Access-Driven Cache Attacks on AES. In: Biham E., Youssef A.M. (eds) Selected Areas in Cryptography. SAC 2006. Lecture Notes in Computer Science, vol 4356. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74462-7_11
24. Gullasch D., Bangerter E. and Krenn S., "Cache Games -- Bringing Access-Based Cache Attacks on AES to Practice," 2011 IEEE Symposium on Security and Privacy, 2011, pp. 490-505, doi: 10.1109/SP.2011.22.
25. Irazoqui G., Inci M.S., Eisenbarth T., Sunar B. (2014) Wait a Minute! A fast, Cross-VM Attack on AES. In: Stavrou A., Bos H., Portokalidis G. (eds) Research in Attacks, Intrusions and Defenses. RAID 2014. Lecture Notes in Computer Science, vol 8688. Springer, Cham. https://doi.org/10.1007/978-3-319-11379-1_15
26. Carmon E., Seifert J. and Wool A., "Photonic side channel attacks against RSA," 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017, pp. 74-78, doi: 10.1109/HST.2017.7951801.
27. Shor. P. W. (1994) Algorithms for quantum computation: discrete logarithms and factoring, Proceedings 35th Annual Symposium on Foundations of Computer Science pp. 124-134.
28. 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
29. Buchmann J., Dahmen E., Klintsevich E., Okeya K., Vuillaume C. (2007) Merkle Signatures with Virtually Unlimited Signature Capacity. In: Katz J., Yung M. (eds) Applied Cryptography and Network Security. ACNS 2007. Lecture Notes in Computer Science, vol 4521. Springer, Berlin, Heidelberg
30. Merkle. R. (1979) Secrecy, authentication and public key systems / A certified digital signature Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University.
31. Aoki K., Guo J., Matusiewicz K., Sasaki Y., Wang L. (2009) Preimages for Step-Reduced SHA-2. In: Matsui M. (eds) Advances in Cryptology – ASIACRYPT 2009. ASIACRYPT 2009. Lecture Notes in Computer Science, vol 5912. Springer, Berlin, Heidelberg
32. Gagnidze A., Iavich M., Iashvili G. (2017) Analysis of Post Quantum Cryptography use in Practice, Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 2, pp. 29-36.
33. Buchmann J., García L.C.C., Dahmen E., Döring M., Klintsevich E. (2006) CMSS – An Improved Merkle Signature Scheme. In: Barua R., Lange T. (eds) Progress in Cryptology - INDOCRYPT 2006. INDOCRYPT 2006. Lecture Notes in Computer Science, vol 4329. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11941378_25

34. Buchmann J., Dahmen E., Klintsevich E., Okeya K., Vuillaume C. (2007) Merkle Signatures with Virtually Unlimited Signature Capacity. In: Katz J., Yung M. (eds) Applied Cryptography and Network Security. ACNS 2007. Lecture Notes in Computer Science, vol 4521. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-72738-5_3
35. A. Shoufan and N. Huber, "A fast hash tree generator for Merkle signature scheme," Proceedings of 2010 IEEE International Symposium on Circuits and Systems, 2010, pp. 3945-3948, doi: 10.1109/ISCAS.2010.5537673.
36. El Bansarkhani R., Misoczki R. (2018) G-Merkle: A Hash-Based Group Signature Scheme from Standard Assumptions. In: Lange T., Steinwandt R. (eds) Post-Quantum Cryptography. PQCrypto 2018. Lecture Notes in Computer Science, vol 10786. Springer, Cham. https://doi.org/10.1007/978-3-319-79063-3_21
37. Buchmann J., García L.C.C., Dahmen E., Döring M., Klintsevich E. (2006) CMSS – An Improved Merkle Signature Scheme. In: Barua R., Lange T. (eds) Progress in Cryptology - INDOCRYPT 2006. INDOCRYPT 2006. Lecture Notes in Computer Science, vol 4329. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11941378_25
38. Iavich, M., Gagnidze, A., Iashvili, G., Hash based digital signature scheme with integrated TRNG, CEUR Workshop Proceedings, 2018
39. Merkle R.C. (1990) A Certified Digital Signature. In: Brassard G. (eds) Advances in Cryptology — CRYPTO' 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. Springer, New York, NY. https://doi.org/10.1007/0-387-34805-0_21
40. Buchmann J., Dahmen E., Schneider M. (2008) Merkle Tree Traversal Revisited. In: Buchmann J., Ding J. (eds) Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science, vol 5299. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88403-3_5
41. Szydlo M. (2004) Merkle Tree Traversal in Log Space and Time. In: Cachin C., Camenisch J.L. (eds) Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24676-3_32
42. Jakobsson M., Leighton T., Micali S., Szydlo M. (2003) Fractal Merkle Tree Representation and Traversal. In: Joye M. (eds) Topics in Cryptology — CT-RSA 2003. CT-RSA 2003. Lecture Notes in Computer Science, vol 2612. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36563-X_21
43. D. Naor, A. Shenhav and A. Wool, "One-Time Signatures Revisited: Practical Fast Signatures Using Fractal Merkle Tree Traversal," 2006 IEEE 24th Convention of Electrical & Electronics Engineers in Israel, 2006, pp. 255-259, doi: 10.1109/EEEI.2006.321066.
44. D. Gottesman, H. -. Lo, N. Lutkenhaus and J. Preskill, "Security of quantum key distribution with imperfect devices," *International Symposium*

onInformation Theory, 2004. ISIT 2004. Proceedings., 2004, pp. 136-, doi: 10.1109/ISIT.2004.1365172.
45. Liao, SK., Cai, WQ., Liu, WY. *et al.* Satellite-to-ground quantum key distribution. *Nature* **549,** 43–47 (2017). https://doi.org/10.1038/nature23655
46. 47 Lo, HK., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nature Photon* **8,** 595–604 (2014). https://doi.org/10.1038/nphoton.2014.149
47. 48 Grosshans, F., Van Assche, G., Wenger, J. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421,** 238–241 (2003). https://doi.org/10.1038/nature01289
48. 49 Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
49. 50 Bouwmeester D, Ekert A and Zeilinger A 2000 *The Physics of Quantum Information* (Berlin: Springer)
50. 51 Fabian Beutel, Helge Gehring, Martin A. Wolff, Carsten Schuck, Wolfram Pernice. (2021) Detector-integrated on-chip QKD receiver for GHz clock rates. *npj Quantum Information* **7**:1, 40. Online publication date: 23-Feb-2021.
51. Lucamarini, M., Yuan, Z.L., Dynes, J.F. *et al.* Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557,** 2018. https://doi.org/10.1038/s41586-018-0066-6
52. Inamori, H., Lütkenhaus, N. & Mayers, D. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D* **41,** 599 (2007). https://doi.org/10.1140/epjd/e2007-00010-4
53. Broadbent, A., Schaffner, C. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.* **78,** 351–382 (2016). https://doi.org/10.1007/s10623-015-0157-4
54. Bennett Ch H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)
55. Bennett Ch H, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography J. Cryptol.
56. Ribordy G, Gautier J-D, Gisin N, Guinnard O and Zbinden H 2000 Fast and user-friendly quantum key distribution J. Mod. Opt.
57. Bethune D and Risk W 2000 An auto-compensating fiber-optic quantum cryptography system based on polarization splitting of light IEEE J. Quantum Electron.
58. Zbinden H, Gisin N, Huttner B, Muller A and Tittel W 2000 Practical aspects of quantum cryptographic key distribution J. Cryptol. 13
59. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509,** 475–478 (2014).

60. Sibson, P., Erven, C., Godfrey, M. *et al.* Chip-based quantum key distribution. *Nat Commun* **8,** 13984 (2017). https://doi.org/10.1038/ncomms13984
61. Lo, HK., Chau, H. & Ardehali, M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *J Cryptology* **18,** 133–165 (2005). https://doi.org/10.1007/s00145-004-0142-y
62. Takeoka, M., Guha, S. & Wilde, M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat Commun* **5,** 5235 (2014). https://doi.org/10.1038/ncomms6235
63. Acín, A., Gisin, N., Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett. 97*, 120405 (2006)