Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 27-38 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

BB84 PROTOCOL AS A PROTOCOL FOR QUANTUM KEY DISTRIBUTION (QKD).

Giorgi Labadze Georgian Technical University

ABSTRACT: The publication of the BB84 protocol by Bennett and Brassard in 1984 marks the beginning of quantum key distribution. Since then, many other protocols have been invented. Yet, BB84 keeps a privileged place in the list of existing protocols: it is the one of the most analyzed and most often implemented, including those used in commercial products. We offer the analysis of BB84 protocol. The physical implementation of the protocol is investigated. Finally, we analyze the eavesdropping strategies against BB84 and deduce the secret key rate.

KEYWORDS: *quantum kay, secret key*

1. შესავალი

BB84 პროტოკოლის პრაქტიკული რიალიზაცია ტექნიკური გამოწვევაა.
სიგნალის წამმოება მაგალითად ფოტონი-არ არის მარტივი ამოცანა. თუმცა ბოლო მიღწევები აჩვენებს, რომ BB84 შესაძლებელია რიალიზებული იქნას თანამედროვე ტექნოლოგიების ეპოქაში.
BB84 პროტოკლში ინფორმაციის საუკეთესო მატარებლებათ ითვლება ფოტონი და მისი ერთი მდგომარეობა. ამასთან უნდა აღინიშნოს წარმოებასთან დაკავშირებით არის სირთულეები და ალტერნატიულ გამოსავალი არის გამოვიყენეოთ სუსტი კონგერენტული მდგომარეობები დაბალი საშვალო რაოდენობის ფოტონებით. მიახლოებით ერთფოტონური მდგომარეობის, სუსტი კონგერენტული მდგომარეობა შეიძლება მოცავდეს ერთზე მეტ ფოტონს, ამ მდგომარეობის ალბათობა შესაძლებელია გაკონტროლებული იქნას. გარდა ამისა დაკარგული ფოტონის წყვილი შესაძლებელია გამოყენებული იქნას ინფორმაციის მატარებლის წარმოებისთვის [1-3].

ფოტონები შესაძლებელია გაგზავნილი იქნას ან ოფტკური არხის დახმარებით ან უკაბელო ქსელით, ეს დამოკიდებულია თუ რას მოითხოვს გარემო პირობები. უნდა აღინიშნოს რომ ოფტიკურ ბოჭკოვაბი კავშირი უნდა ინეს უპირატესად მიჩნეული ტელეკონუნიკაციური ქსელისთვის.

ქუბიტი კოდირება შესაძლებელია შესრულებული იქნას ფოტონის პოლარიზაციით ან მისი ფაზით. ფაზირებული კოდირება ძირითადათ უკეთესია ფოტონებისთვის.

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. კვანტურ მატარებელს BB84 - ს ვერ აღვწერთ კლასიკური ტერმინებით, ამიტომ ჩვენ უნდა მოვახერხოთ ჩვენი ენის ადაპტაცია ამ ახალ პარამეტრთან. არსებობს შესაბამისობა ზოგიერთი ფიზიკური სისტემის კვანტურ მდგომარეობასა და მის მატარებელ ინფორმაციას შორის.

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

კვანტურ თეორიაში 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.

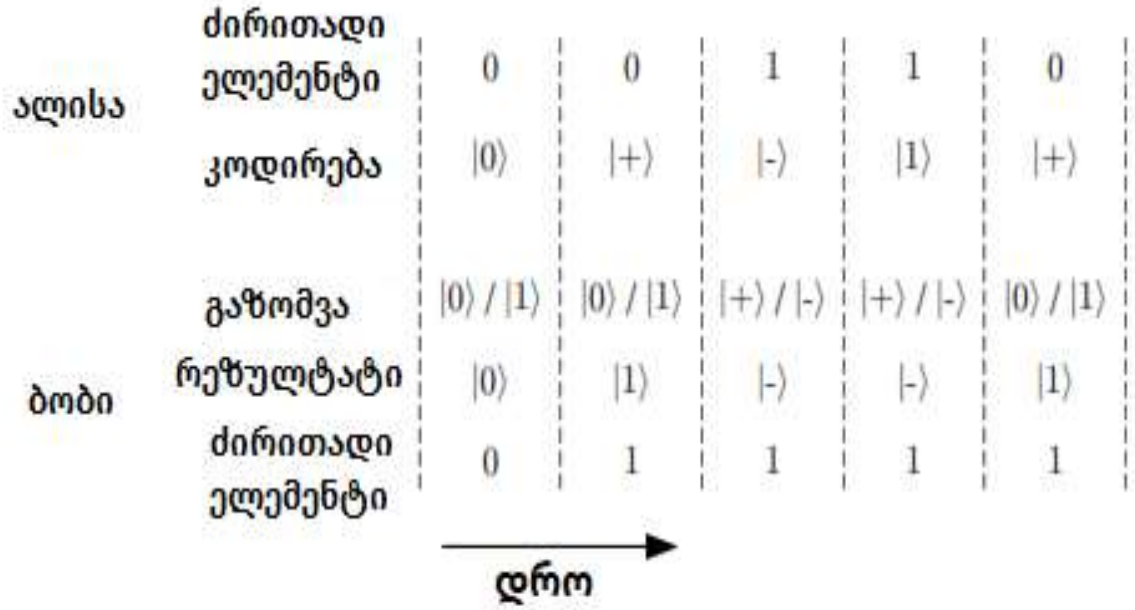
$$\{\alpha|0\rangle + \beta|1\rangle : \ |\alpha|^2 + |\beta|^2 = 1 \ \ \alpha, \beta \in C\}$$

ორი საბაზო ქუბიტი, რომელიც შესაბამება ორ ორთოგონალურ მდგომარეობას კვანტურ სისტემაში. ქუბიტებს $|0\rangle$ $(\alpha = 1, \beta = 0)$ 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 ალისა 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 ალისა 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 ალისამ 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 $\alpha\alpha' * + \beta\beta' * = 0$.

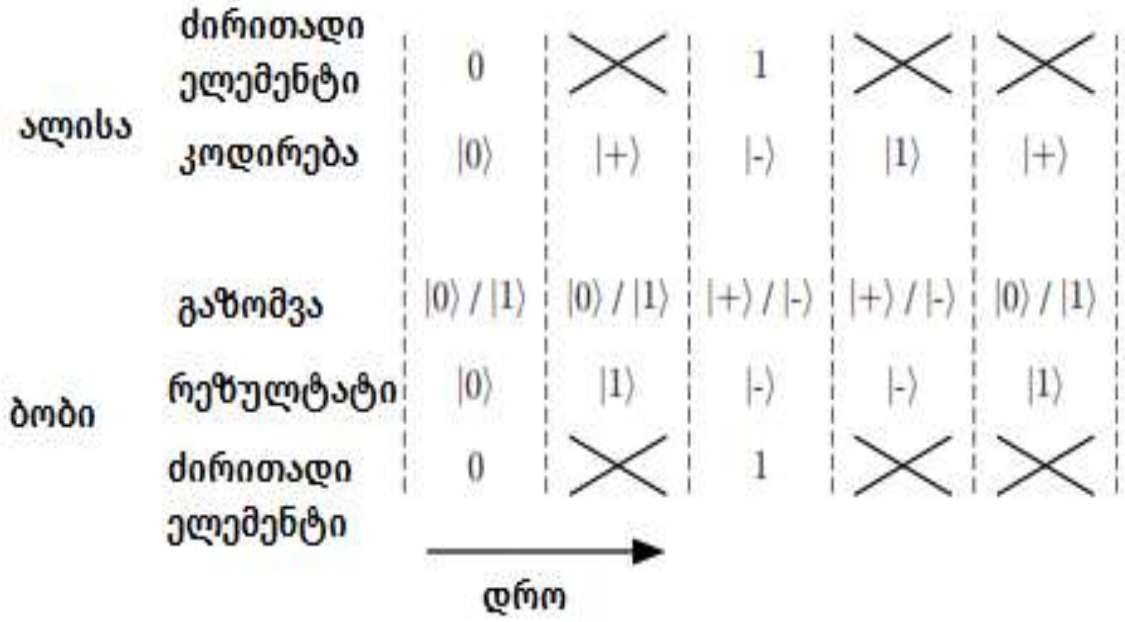
მაგალითად ავიღოთ ორთოგონალური ქუბიტები $|0\rangle$ და $|1\rangle$. ბობს შეუძლია ჩაატაროს გაზომვები რომელიც გაარკვევს ალისას გამოგზავნილი $|0\rangle$ ან $|1\rangle$. მაგრამ რა ხდება თუ ის აგზავნის $|+\rangle$ ან $|-\rangle$? ფაქტობრივად , ბობი იღებს რეზულტატს შემთხვევით! ზოგადად თუ ბობი მიიღებს $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ 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 არაკორერილებუ ბიტების მნიშვნელობას. რა არის განსაკუთრებული ქუბიტებში $|0\rangle$ და $|1\rangle$ შეძლება ევივალენტურად 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 ალისას შეტყობინების დეკოდირება როცა ის აგზავნის $|+\rangle$ და $|-\rangle$, მაგრამ ის ვერ შეძლებს გაარჩიოს $|0\rangle$ და $|1\rangle$. ტრანსმიის დედექციის მაგალითი მოცემულია ნახაზი 1.2-ზე.

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



ნახაზი 1.2 ტრანსმისიის მაგალითი BB84 გამოყენებით. პირველი ორი სტრიქონი არის რას აგზავნის ალისა. მესამე სტრიქონი გვაჩვენებს ბობის მიერ არჩეულ გაზომვის მეთოდს და გაზომვის შედეგად მიღებულ შესაძლო რეულტატს [4-6].

ალისამ აირჩია ყველა ძირითადი ელემენტი , ახლა ბობს შეუძლია გადაყაროს ყველა არასწორი გაზომვა; პროტოკოლის ამ ნაწილს ეწოდება გაცრა (ე.წ. შიფტინგი) რომელიც ნაჩვენებია ნახაზი 1.3-ზე



ნახაზი 1.3 ნახაზი 1.2 ტრანსმისიის შიფტინგი, ძირითადი ელემენტები რომლისთვისაც ბობის გაზომვები არ ემთხვევა ალისას კოდირების წესი იყრება.

ჯერჯერობით რომ შევაჯამოთ, ალისა უგზავნის ბობს შემთხვევით ბიტებს. ალისა ირჩევს ოთხი განსხვაბევული ქუბიტისგან ბიტების კოდირებისთვის (ორი სავარაუდო ქუბიტი ბიტზე). ბობი ირჩევს ორი გაზომვის მეთოდიდან ერთ-ერთს დეკოდირებისთვის. ბობს ყოველთვის არ შეუძლია დეტერმინირება რა გაუგზავნა ალისამ, მაგრამ გაცრის(შიფტინგის) შემდგომ ალისა და ბობი ინახავენ ბიტების უმრავლესობას რომელთათვისაც ტრანსიმისია წარმატებით განხორციელდა. ტრანსმისის ეს სქემა ალისას და ბობს აძლევს საშალებას შეამჩნიონ მოსმენა.

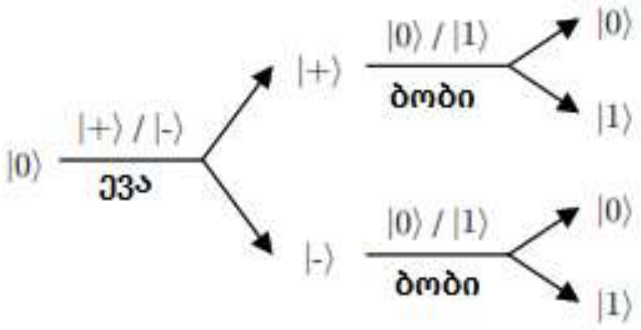
2.მოსმენის ამოცნობა

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

კვანტურ მექანიკაში გაზომვები დესტრუქციულია. ნაწილაკის გაზომვის შემდეგ, რეზულტატს ვიღებთ როგორც მდგომარეობას. უფრო ზუსტად, 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 $|\phi\rangle \rightarrow |\phi'\rangle = |1\rangle$, 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 ალისას 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. მაგრამ 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 1.4 -ზე. არასწორ მდგომარეობაში ბობი ძირითადად ზომავს შემთხვევით ბიტს, რომელსაც აქვს ალბათობა ½ დამთხვევის ალისას ბიტთთან და ალბათობა ½ შეცდომის.



ნახაზი 1.4 შესაძლო შედეგები როცა ევა იყენებს არასწორ გაზომვებს მოსმენისათვის

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 ნიმუშს არ გამოყენებენ ალისა და ბობი გასაღების დასამზადებლად. თუმცა, თუ ის მაინც მოახდენს მდგომარეობების რეტრანსლირებას (მიუხედავად იმისა, რომ ის არასწორია ½ შემთხვევაში), ალისა და ბობი

აღმოაჩენენ მის არსებობას, უჩვეულოდ დიდი რაოდენობის შეცდომების გამო მათ ძირითად ელემენტებში.

ბობს და ევას აქვთ ერთი და იგივე სირთულე, ალისას გამოგზავნილ ინფორმაციასთან მიმართებაში, რადგან მათ არ იციან კოდირების რომელი წესია გამოყენებული. მაგრამ სიტუაცია არ არის სიმეტრიული ბობისთვის და ევასთვის: ყველა კომუნიკაცია, აუცილებელია შიფტინგის შესასრულებლად , კლასიკურ აუთენთიფიცირებულ არხში. ეს საშუალებას აძლევს ალისას გაარკვიოს, რომ ესაუბრება ბობს და არა ევას. შესაბამისად, კანონიერი მხარეები იძლევა იმის გარანტიას რომ შიფტინგის პროცესზე ევა ვერ იქონიებს გავლენას. ამრიგად ალისას და ბობს შეუძლიათ მხოლოდ ის ძირითადი ელემენტები შეადარონ რომელიც სწორად გაიზომა. მსმენელის არსებობის დასადგენად , ალისას და ბობს უნდა ქონდეთ საშუალება ტრანსმისიის შეცდომების აღმოჩენის. ამისთვის არის საშუალება გავხსნათ ნაწილი გაცრილი გასაღების. მოცემულ პროტოკოლს შეუძლია ტრანსმისიის შემდეგ აჩვენოს $l + n$ ძირითადი ელემენტი(მაგალითად., l+n =100 000) ინდექსირებული 0 დან l+n -1, ალისა შემთხვევით ირჩევს n ინდექსს (მაგალითად n= 1000) შემდეგ ახდენს კომუნიკაციას ბობთან. შემდეგ ალისა და ბობი ხსნიან შესაბამის n 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. რა თქმა უნდა მაშინ დარჩენილი ძირითადი ელემენტები იქნება გამოყენებული საიდუმლო გასაღების შესაქმნელად.

3.საიდუმლო გასაღების შექმნა.

იმ შემთხვევაში, თუ შეცდომები გამოვლინდა, ალისას და ბობს შეუძლიათ გაწყვიტონ პროტოკოლი, რადგან შეცდომები შეძლება გამოწვეული იქნას მოსმენისგან. უკიდურეს შემთხვევაში ეს ხელს უშლის გასაღების შექმნას, რომელიც შეიძლება ცნობილი გახდეს მოწინააღმდეგისთვის. გადაწყვეტილების ეს მხარე შეიძლება იყოს ცოტათი მკაცრი. პრაქტიკაში ფიზიკური რეალიზაცია არ არის იდეალური, რადგან შეცდომები შეიძლება

გამოწვეული იქნას ბევრი მიზეზით, გარდა მოსმენისა, ისეთი როგორიცაა მაგალითად ხმაური ან კვანტურ არხში დაკარგვა, არასრული გენერაცია კვანტური მდგომარეობის ან არასრული დედექცია. ასევე, ევამ შეიძლება მოისმინა პატარა ნაწილი დაშიფრული გასაღების, შექნას გასაღების დარჩენილი ელემენტები, საიდუმლო გასაღების შესაქმნელად. შესაბამისად უნდა გამოინახოს გზა შეიქმნას კვანტური გასაღების პროტოკოლი უფრო მდგრადი ხმაურთან მიმართებაში.

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

ამ ეტაპზე ალისამ და ბობმა იციან, რომ გახსნილ ძირითად ელემენტებს აქვთ e შეცდომების ნორმა და პოტენციური მსმენელს აქვს I_E ინფორმაცია მათზე. კლასიკური საერთო აუთენთიფიცირებული არხით , ალისას და ბობს შეუძლათ კიდევ სცადონ შექმნან სრულად საიდუმლო გასაღები; ამ ნაწილს ეწოდება საიდუმლო გასაღების დისტილაცია.

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

BB84 შემთხვევაში, შეთანხმება ჩვეულებრივ იღებს ინტერაქტიულ სახეს, შეცდომების შეასწორებს პროტოკოლი. ალისა და ბობბი ალტერნატიულად ამჟღავნებენ მათი ძირითადი ელემენტების ტოლ ქვესიმრავლეებს. როდესაც ისინი აღმოაჩენენ თანაფარდობის სხვაობას, ეს ნიშნავს, რომ შესაბამისი ქვესიმრავლეები შეიცავს გაურკეველი რაოდენობის შეცდომებს. უკიდურეს შემთხვევაში ერთს მაინც. დიხოტომიის გამოყენებით მათ შეუძლიათ შეცდომის ადგილმდებარეობის დაფიქსირება და მისი შესწორება. ისინი იმეორებენ ამ პროცეს საკმარისი რაოდენობით და შედეგად ალისა და ბობი ცვლიან ტოლ ბიტებს.

საიდუმლო გასაღების დისტილაციისას , ყველა კომუნიკაცია ხდება საერთო აუთენთიფიცირებული კლასიკური არხით. დავიმახსოროთ, რომ ევას არ შეუძლია ინტერვენცია ამ პროცესში, მაგრამ მას შეუძლია მოუსმინოს გაცვილილ შეტყობინებებს. რომელიც ამ შემთხვევაში შეიცავს გაცვლილ თანაბარ ბიტებს. მაშასადამე, ევას ცოდნა მოიცავს $I_E + |M|$ ბიტს, $|M|$ მნიშვნელობის თანაბარი ბიტებით, რომელიც შესწორებისას იქნა აღმოჩენილი. იმისთვის, რომ გასაღები იყოს საიდუმლო, კონფიდენციალურობის გაძლიერების იდეა მდგომარეობს იმაში, რომ გამოვიყენოთ ის რაც არ იცის ევამ. ალისას და ბობს შეუძლიათ დაითვალონ გასაღების ელემენტების ფუნქცია f-ი, ისე რომ გაავრცელონ ნაწილობრივი ევას უცოდინაროზა მთელ რეზულტატზე. ასეთი ფუნქცია (მაგალითად, როგორც ჰეშ ფუნქცია კლასიკურ კრიფტოგრაფიაში) ირჩევა ისე რომ თითეული გამომავალი ბიტი დამოკიდებულია შემავალი ბიტების უმეტეს ნაწილზე თუ არა ყველაზე. მაგალითად, ასეთი ფუნქცია შედგება თანაბარი შემთხევითი ქვესიმრავლეების ბიტების გამოთვლით. დავუშვათ, 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 მნიშვნელობა , 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 კონფიდენციალურობის გასამყარებლად არის ის , რომ გამომავალი საიდუმლო გასაღების სიგრძე უნდა იყოს ნაკლები, ვიდრე შემავალი ნაწილობრივ საიდუმლო გასაღების სიგრძე. შემოკლების ზომა დაახლოებით ტოლია ბიტების იმ რაოდენობისა რაც იცის ევამ და გასაღების ზომის რეზულტატი $l - I_E -$

$|M|$ ბიტებში. გასაღების მაქსიმალური ზომის მღება შესლებელია როცა ევამ არი იცის არაფერი გასაღების შემადგენელ ბიტებზე და (მაგალითად $l - I_E - |M| = 0$). მნიშვნელოვანია რომ გამოხშირვა , შესაძლებობის ფარგლებში ხსნიდეს მაქსიმალურად ნაკლებ ინფორმაციას, საკმარისს იმისთვის, რომ ალისამ და ბობმა შეძლონ შეასწორონ ყველა შეცდომა. მივაქციოთ ყურადღება იმას, რომ საიდუმლო გასაღების ნაწარმოები ბიტების რაოდენობიდან უხეშად რომ ვთქვათ, კვანტური გადაცემისას შეცდომების გასწორება გვიწევს ორჯერ. პირველ რიგში შეცდომები უნდა მივაკუთნოთ მოსმენას და I_E ჩავთვალოთ. ასევე , შეცდომები უნდა იქნას სწრაფად გამოსწორებული, რისთვისაც ბიტების ნაწილი უნდა იქნას გახსინილი და ჩაითვალოს $|M|$.

საბოლოოდ, საიდუმლო გასაღები, მიღებული კომფედენციალურობის გაძლიერების შემდგომ, ალისას და ბობს შეუძლიათ გამოიყენონ კრიფტოგრაფიული მიზნებისთვის. კერძოდ, მათ შეუძლიათ გასაღების გამოყენება შეტყობინების დასაშიფრად ან საიდუმლო არხის შესაქმნელად.

ბიბლიოგრაფია

1. Li, HW., Yin, ZQ., Wang, S. *et al.* Randomness determines practical security of BB84 quantum key distribution. *Sci Rep* 5, 16200 (2015). https://doi.org/10.1038/srep16200
2. Zhizhong Yan, Evan Meyer-Scott, Jean-Philippe Bourgoin, Brendon L. Higgins, Nikolay Gigov, Allison MacDonald, Hannes Hübel, and Thomas Jennewein, "Novel High-Speed Polarization Source for Decoy-State BB84 Quantum Key Distribution Over Free Space and Satellite Links," J. Lightwave Technol. 31, 1399-1408 (2013)
3. Chen, F.-L.; Wang, Z.-H.; Hu, Y.-M. A New Quantum Blind Signature Scheme with BB84-State. Entropy 2019, 21, 336. https://doi.org/10.3390/e21040336
4. S. Gnatyuk, T. Okhrimenko, M. Iavich and R. Berdibayev, "Intruder Control Mode Simulation of Deterministic Quantum Cryptography Protocol for Depolarized Quantum Channel," *2019 IEEE*

International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019, pp. 825-828, doi: 10.1109/PICST47496.2019.9061293.

5. Hu, S. Gnatyuk, T. Okhrimenko, V. Kinzeryavyy, M. Iavich, Kh. Yubuzova, High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits, CEUR Workshop Proceedings, Vol. 2393, pp. 810-821, 2019.

6. J. Huang, Y. Wang, H. Wang, Z. Li and J. Huang, "Man-in-the-middle attack on BB84 protocol and its defence," *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 2009, pp. 438-439, doi: 10.1109/ICCSIT.2009.5234678.