ПРИМЕНА ДЕТЕКТОВАЊА ПОЛАРИЗАЦИЈЕ ФОТОНА У ПРОТОКОЛИМА КВАНТНЕ КРИПТОГРАФИЈЕ СИМУЛИРАНА У CRYPTOOL

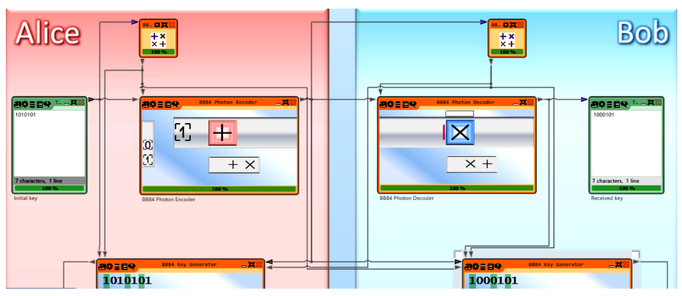
Хана Стефановић[1], Никола Давидовић[2], Верица Васиљевић[3] ,Слободан Обрадовић[1]
1) Висока школа струковних студија за ИТ, Београд, Србија
2) Универзитет у Источном Сарајеву, Електротехнички факултет, Источно Сарајево, РС, БиХ
3) ФИТ Слободан П. Универзитета,Бијељина,РС,БиХ

Сажетак: У раду су примењени неки принципи квантне криптографије и квантне размене кључа (QKD – Quantum Key Distribution) који се ослањају на трансмисију фотона кроз оптичка влакна, користећи стања поларизације фотона, у простору квантних стања фотона. Шема кодирања и квантни алфабет, са квантним стањима која граде коњуговане базе, имплементирани су према спецификацијама протокола BB84 и симулирани у софтверском алату Cryptool.

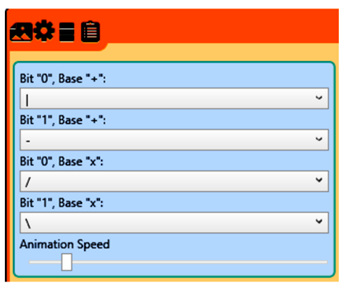
Савремено пословање, које се пре свега заснива на употреби рачунарских система и размени података у електронском облику, изложено је различитим ризицима који могу имати несагледиве последице. Напади на рачунарске мреже, покушаји неовлашћеног приступа подацима, прислушкивање или надгледање протока података, као и злонамерне измене података свакодневна су појава. Напредак технологије омогућио је примену нових начина комуникације, омогућено је лакше пословање, али се истовремено појавио и проблем сигурности, као и потреба за увођењем нових механизама који треба да преузму улогу класичних питања и решења као што су идентификација, контрола приступа и верификација. Одговоре на већину оваквих изазова нуди примена криптографских решења, мада постоје проблеми на која криптографија не може адекватно да одговори

Квантна криптографија, односно квантна дистрибуција кључа (QKD – Quantum Key Distribution) ослања се на квантну механику, управо са циљем да се реализује безбедна комуникација. Потребно је да два корисника који комуницирају (особа А – Алиса и особа Б – Боб) креирају заједнички насумични низ битова познат само њима, а који се може даље користити као кључ за шифровање и дешифровање порука, применом неког од алгоритама класичне или модерне криптографије. Квантна криптографија у том смислу има улогу у креирању и сигурној размени кључа, а принципи кватне механике омогућавају учесницима да уоче присуство треће особе која покушава да открије информације о кључу

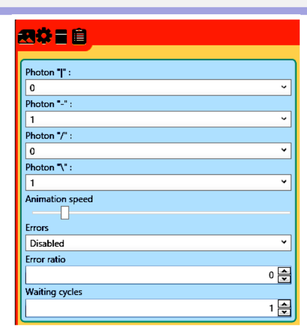
У симулационом моделу, имплементираном у софтверском алату Cryptool, као што је приказано на Сл. 1, коришћена су стања горе, доле, лево и десно, као што је илустовано на Сл. 2. Четири квантна стања граде две базе, које су максимално коњуговане. Мапирање квантних стања у одговарајуће битске вредности дато је на Сл. 3.



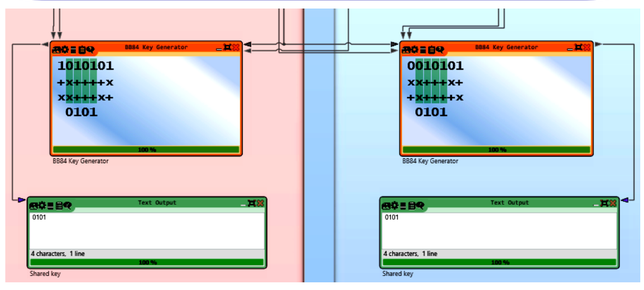
Слика 1. Модел квантног комуникационог система (пошиљалац Алиса, прималац Боб)



Слика 2. Мапирање квантних стања према одговарајућим базама



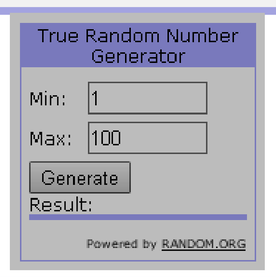
Слика 3. Мапирање квантних стања у одређене бинарне вредности



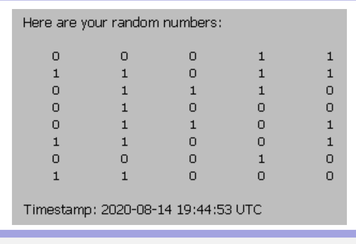
Слика 4. Формирање просејаног кључа (Shared key)

На Сл. 3. приказано је мапирање квантних стања у одређене бинарне вредности, за изабрани симулациони модел, док је мапирање квантних стања према одговарајућим базама дато на Сл. 2. У предложеном слимулационом моделу, линеарно хоризонтално и дијагонално стање под углом од 135° одговарају јединици, док линаерно вертикално и дијагонално под углом од 45° одговарају нули.
Као разултат добија се заједнички просејани кључ, који је приказан на Сл. 4. На овај начин Алиса и Боб могу генерисати онолико битова колико им је потребно за кључ који ће се даље користити у процесу шифровања и дешифровања.
У просеку, Боб погађа исправну поларизацију у 50% случајева, тако да је и просејани кључ у просеку 50% краћи у односу на дужину полазне секвенце. Размена битова између Алисе и Боба, са одговарајучим кодирањима, за различите начине оријентације филтара,

У случају постојања трећег лица – прислушкивача, Алиса и Боб ће бити у могућности да то примете, а због самих принципа квантне криптографије. Прислушкивач (Ева) такође мора да погађа поларизације приликом мерења, и такође ће имати добре претпоставке у просеку у 50% случајева. Међутим, тиме ће бити промењена и стања поларизованих импулса, услед чега би Алиса и Боб добили различите низове, што је индикатор постојања прислушкивача. Уобичајено је део кватног протокола и поређење неколико битова почетне секвенце, управо да би се открило потенцијално присуство прислушкивача. Такви тест битови се касније одбацују и не учествују у формирању просејаног кључа.



Слика 5. Генератор случајних бројева који користи податке о атмосферском шуму



Слика 6. Генерисање низа битова случајних вредности употребом True Random Number генератора

Даље унапређење модела симулираног у овом раду односило би се на употребу генератора случајних бројева (True Random Number Generator) који користи податке о атмосферском шуму [12], као што је приказано на Сл. 5 и Сл. 6. Овакав генератор има много боље карактеристике [13] од псеудослучајног генератора доступног у Cryptool алату, а који је коришћен у приказаним симулацијама.
Избор једне од две расположиве базе поларизације на предајној и на пријменој страни треба да буде случајан, а свака псеудослучајност деградира сигурност комуникационог протокола, тако да би употреба оваквог генератора допринела побољшању перформанси анализираног модела. Одговарајућим подешавањима могуће је генерисати потребан број случајних битова, који би одредили избор базе поларизације на предајној и пријемној страни, као што је илустровано на Сл. 6.

Комуникациони квантни модел система симулираан у овом раду, ослањајући се на основне принципе BB84 протокола, обезбеђује генерисање тајног просејаног кључа за учеснике у комуникацији, који даље може бити коришћен као кључ у неким класичним алгоритмима за шифровање и дешифровање. За квантну дистрибуцију кључа коришћена су два неортогонална квантна стања, услед чега треће лице у улози прислушкивача не може недвосмислено и без деградирања оригиналног стања квантног система да разликује два квантна стања која пошиљалац користи за представљање битова које шаље примаоцу, с обзиром да су та квантна стања неортогонална.

ЛИТЕРАТУРА
[1] M. Stamp, Information Security: Principles and Practice, JohnWiley & Sons, 2006.
[2] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics 8 (2014) 595–604.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74 (2002) 145–195.
[4] Y. Nambu, K. Yoshino, and A. Tomita, Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit, J. Mod. Opt. 55 (2008) 1953–1970.
[5] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature 299 (1982) 802–803.
[6] https://www.cryptool.org/en/
[7] C. Bennett and G. Brassard, Quantum Cryptography: public key distribution and coin tossing, in Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (1984) 175–179.
[8] Y. Nambu, T. Hatanaka, and K. Nakamura, BB84 quantum key distribution system based on silica-based planar lightwave circuits, Jpn. J. Appl. Phys. 43 (2004) L1109– L1110.
[9] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2000) 441–444.
[10] https://www.idquantique.com/
[11] https://www.idquantique.com/random-number-generation/overview/
[12] https://www.random.org/
[13] https://www.random.org/#numbers