ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – ВАРНА
ФАКУЛТЕТ ПО ИЗЧИСЛИТЕЛНА ТЕХНИКА И АВТОМАТИЗАЦИЯ
КАТЕДРА КОМУНИКАЦИОННА ТЕХНИКА И ТЕХНОЛОГИИ

инж. Георги Петров Бебров

АВТОРЕФЕРАТ

на дисертация за получаване на образователна и научна степен „доктор“
на тема

МЕТОДИ ЗА ПОВИШАВАНЕ ЕФЕКТИВНОСТТА НА МОДЕЛИ ЗА КОНФИДЕНЦИАЛНИ КВАНТОВИ КОМУНИКАЦИИ

по докторска програма „Комуникационни мрежи и системи“ към
професионално направление 5.3. „Комуникационна и компютърна техника“

Научен ръководител: проф. д-р инж. Розалина Стефанова Димова

Рецензенти:

1. .....
2. .....

Варна, 2020

Дисертационният труд е обсъден на 01.12.2020г. в катедра “Комуникационна техника и технологии” и насочен за защита.

Докторантът работи в катедра “Комуникационна техника и технологии”.

Автор: инж. Георги Петров Бебров

Заглавие: Методи за повишаване ефективността на модели за конфиденциални квантови комуникации

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – ВАРНА
ФАКУЛТЕТ ПО ИЗЧИСЛИТЕЛНА ТЕХНИКА И АВТОМАТИЗАЦИЯ
КАТЕДРА КОМУНИКАЦИОННА ТЕХНИКА И ТЕХНОЛОГИИ

инж. Георги Петров Бебров

АВТОРЕФЕРАТ

на дисертация за получаване на образователна и научна степен „доктор“
на тема

МЕТОДИ ЗА ПОВИШАВАНЕ ЕФЕКТИВНОСТТА НА МОДЕЛИ ЗА КОНФИДЕНЦИАЛНИ КВАНТОВИ КОМУНИКАЦИИ

по докторска програма „Комуникационни мрежи и системи“ към
професионално направление 5.3. „Комуникационна и компютърна техника“

Варна, 2020

Дисертационният труд съдържа 184 страници. Оформен е в 4 глави, общи изводи и списък на използваната литература от 136 заглавия, като всички са на латиница.

Защитата на дисертационния труд ще се състои на 02.04.2021г. в Конферентна зала НУК, ТУ-Варна на открито заседание на жури, сформирано със заповед на Ректора №560/14.12.2020г.

Материалите по защитата (дисертацията, рецензиите и становищата) са на разположение на интересуващите се в Докторантски център, стая 318 НУК.

Благодарности

Авторът изказва искрени благодарности за участието си в проект „ДН07/10 - „Изследване на архитектури, модели и методи за автономен мениджмънт в интернет на бъдещето – ТУ-София, 2016г.“, подпомагнал реализацията на изследванията, влизащи в състава на настоящия дисертационен труд.

ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Бурното развитие на квантовите компютърни технологии, които включват квантовите компютри, квантовия изкуствен интелект и квантовите алгоритми, довеждат до напредък в методите за криптоанализ. Неразривната връзка между криптоанализа и криптографията налага от своя страна и развитието на последната. Решението за противопоставяне на квантовите компютърни технилогии е т.нар. квантова криптография – научна област, която се занимава с разработването и усъвършенстването на модели за конфиденциален пренос на криптографски ключове.

В настоящето е налице тенденция на квантови модели за пренос на криптографски ключове (КМПКК), която се характеризира със следните обстоятелства:
- стремеж за подобряване на моделите за конфиденциален квантов пренос на криптографски ключове. Това по-обобщено може да се отчете като стремеж за разработване на оптимизиран модел за конфиденциален квантов пренос на криптографски ключове;
- стремеж за реализиране на идеална практическа система за конфиденциален квантов пренос на криптографски ключове.

Разработките в представената дисертационна работа са свързани с първото обстоятелство на гореизложената тенденция: (i) предлагат методи за подобряване ефективността на стандартни модели за конфиденциален квантов пренос на криптографски ключове. Предложените модели се анализират относно тяхната сигурност при интегрирането им към споменатите модели; (ii) предлага се методика за обобщена оценка, наречена *оптималност*, на съществуващите модели за конфиденциален квантов пренос на криптографски ключове.

Цел и задачи на изследването

Цел на дисертационния труд е да се разработят методи за увеличаване ефективността и бързодействието съществуващи КМПКК модели, както и за обобщено оценяване и сравняване на последните.

Спрямо гореизложения анализ, за постигане на поставената цел е необходимо да се решат следните задачи:

(i) да се предложи, изследва, приложи и практически реализира метод за по-ефективно пренасяне на съобщения при определени КМПКК модели.

(ii) да се предложи, изследва и приложи метод за удължаване на криптографския ключ на КМПКК модели.

(iii) да се предложат изрази за оценяване практичността, сигурността и по-коректно ефективността на КМПКК модели.

(iv) да се предложи метод за обобщено оценяване и сравняване на КМПКК модели, което включва ефективността, сигурността и практичността.

Обект и предмет на изследване

Обект на изследването са квантовите методи за пренос на криптографски ключове.

Предмет на изследването са методи за увеличаване на ефективността при КМПКК и метод за обобщена оценка на КМПКК.

Методи на изследване

За описание и анализ на предложените методи се използва математическия апарат на теорията на множествата.

За осъществяването на анализ спрямо сигурността на предложежите методи се използва математическия апарат на теорията на информацията, която от своя страна се базира на теорията на вероятностите.

За провеждане на симулационния анализ за влиянието на предложените методи към сигурността на моделите, към които се интегрират, се използва програмния език C++ - Dev-C++ компилатор.

Място на изследване

Изследванията са проведени в лабораториите на катедра КТТ на Технически Университет – Варна, България.

Научна и практическа новост на изследването

На базата на извършване на задачите, заложени в дисертационния труд, се разграничават следните приноси:

- Предложен е метод за увеличаване на ефективността при преноса на съобщения при модели за конфиденциален квантов пренос на криптографски ключове от по-ефективен тип;
- Предложен е метод за увеличаване на ефективността при установяване на криптографски ключове при моделите за конфиденциален квантов пренос на криптографски ключове;
- Изследва се сигурността, с която се характеризират предложените методи при тяхното интегриране в модели за конфиденциален квантов пренос на криптографски ключове;
- Предложено е устройство, което реализира метода за увеличаване на ефективността при преноса на съобщения;
- Предлага се модел за конфиденциален квантов пренос на криптографски ключове от по-ефективен тип, който се базира на предложения метод за по-ефективен пренос на съобщения;
- Предлага се модел за конфиденциален квантов пренос на криптографски ключове, който се базира на предложения метод за по-ефективно установяване на криптографски ключове;
- Предложен е израз за по-обобщена оценка ефективността на моделите за конфиденциален квантов пренос на криптографски ключове;
- Предложен е израз относно комуникационната продължителност на моделите за конфиденциален квантов пренос на криптографски ключове;
- Извършен е анализ на ефективността на новопредставените модели;
- Предложен е израз за оценка сигурността на моделите за конфиденциален квантов пренос на криптографски ключове;
- Предложен е израз за оценка практичността на моделите за конфиденциален квантов пренос на криптографски ключове;
- Предложен е метод за обобщена оценка на моделите за конфиденциален квантов пренос на криптографски ключове.

Апробация на изследването

Резултатите от дисертационния труд са представени в 7 публикации:

- доклад – OPTIM-ACEMP Conference, Brasow, Romania, 2017.
- публикация – Annual Journal of Technical University of Varna, Vol.1, Issue 1, 2017.
- публикация – International Journal of Theoretical Physics, **59**, 426-435, 2020.
- доклад – BIA Conference, Varna, 2019.
- 2 публикации – The European Physical Journal D
- публикация - Engineering and Technology International Journal of Physical and Mathematical Sciences, Vol.13, No.2, 2019.

Докладите представени на *OPTIM-ACEMP Conference*, *BIA Conference* и публикациите налични в *International Journal of Theoretical Physics*, *The European Physical Journal D* са индексирани в SCOPUS.

СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА I. СЪСТОЯНИЕ НА КВАНТОВИТЕ МОДЕЛИ ЗА ПРЕНОС НА КРИПТОГРАФСКИ КЛЮЧОВЕ. ОБЗОР И АНАЛИЗ НА ЛИТЕРАТУРАТА ДО НАСТОЯЩИЯ МОМЕНТ.

В тази глава са разгледани различните типове на квантови модели за пренос на криптографски ключове (КМПКК) – това са квантови конфиденциални комуникации **ККК** (QSDC/DSQC – quantum secure direct communication/deterministic secure quantum communication) [25-45,76-80,111-114] и квантово разпределение на криптографски ключове **КРКК** (QKD – quantum key distribution) [1-23,49-68,93-98,103-110], както и техни производни подходи, като например *КРКК модел, независещ от използваните устройства* (НУ-КРКК) [4] и *КРКК, независеща от измервателното устройство* (НИУ-КРКК) (англ. Measurement-device-independent quantum key distribution - MDI-QKD) [5-7].

Също така се анализира проблема на КМПКК, който е свързан с ефективността на тези модели. Известно е от литературата [68], че КМПКК се характеризират както с присъщ за тях проблем - наличие на процедури, при които голяма част от използваните ресурси (двоични символи) се отхвърлят, така и с практически проблем – използваните при тях еднофотонни приемници са с ниска скорост на детектиране. Първият проблем води до ниска ефективност, докато вторият до ниска скорост на установяване на криптографски ключове. Съществуващо решение на втория проблем е използването на многонивови квантови системи [68,69]. В дисертационния труд, в Глава II, се предлага решение на първия проблем, с което да се редуцират недостатъците на КМПКК моделите.

Освен това в тази глава се акцентира върху проблема, свързан с обобщеното оценяване на съществуващите КМПКК. Проблемът е в това, че липсва метод за обобщено оценяване на моделите с цел по-добро тяхно сравнение. За тази цел в Глава IV се представя метод, който включва основните параметри на КМПКК – ефективност, сигурност и практичност.

ГЛАВА II. МЕТОДИ ЗА УВЕЛИЧАВАНЕ ЕФЕКТИВНОСТТА НА ДККК И НИУ-КРКК МОДЕЛИ.

В тази глава се представят решения, свързани с проблема за ефективността на моделите ДККК и НИУ-КРКК. Съответно тези решения са описани в т.2.2.1. и т.2.2.2. Освен това се доказва коректността на тези решения спрямо сигурността на горепосочените

квантови модели за пренос на криптографски ключове – потвърждава се, че прилагането на методите не доставя информация за установявания ключ на неоторизирани лица.

2.2. МЕТОДИ ЗА УВЕЛИЧАВАНЕ НА ЕФЕКТИВНОСТТА.

2.2.1. МЕТОД ЗА УВЕЛИЧАВАНЕ НА ЕФЕКТИВНОСТТА НА ККК МОДЕЛ ОТ ДККК ТИП.

Пристъпва се към представянето на метода за увеличаване на ефективността при ККК модел за комуникация. Този метод е наречен *компресията на квантовия канал* (ККвК, на англ. *quantum channel compression* – QCC). Това е процес, при който се кодира двоично съобщение върху квантови системи. ККвК е различно от оптималното кодиране [48]. Това кодиране се характеризира чрез механизъм, който се състои от следните принципи:

Принцип 1. Всеки нечетен двуразреден символ X_p (p = 0,2,..,n-2) на двоична последователност X се кодира върху двуквантова система с максимално корелирани съставни части: ($00 \rightarrow \Phi^+$, $01 \rightarrow \Phi^-$, $10 \rightarrow \Psi^+$, $11 \rightarrow \Psi^-$) – [f: $X_p \rightarrow Q_p$].

Принцип 2. Всеки четен двуразреден символ X_m (m = 1,3,..,n-1) на двоичната последователност X се кодира в поляризационно състояние на елементарна квантова система (V, H, D = (V+H)/√2, A = (V-H)/√2). Състоянието на квантовата система зависи от стойностите на предходния двуразреден символ X_{m-1} и на текущия символ X_m – [f′: $X_m \rightarrow q_m \mid X_{m-1}$]. Този процес се характеризира с таблицата:

Табл.2.1. Кодираща/Декодираща таблица за процеса ККвК.

q_m	X_m	X_{m-1}	q_m	X_m	X_{m-1}
V	00	00	D	00	01
H	01	00	A	01	01
D	10	00	V	10	01
A	11	00	H	11	01
q_m	X_m	X_{m-1}	q_m	X_m	X_{m-1}
H	00	10	A	00	11
V	01	10	D	01	11
A	10	10	H	10	11
D	11	10	V	11	11

За да се декодира еднозначно информацията, пренасяна от елементарната квантова система, спомагателен едноразреден двоичен символ B е нужно да се изпрати заедно с квантовата система (B = 0 – V/H базис, B = 1 – D/A базис).

На езика на теорията на множествата ККвК подходът се описва със следната функция

$$F: \{0,1\}^4 \in GF(2^4) \rightarrow [\{|\Psi>\} \in (\mathbb{H}_1 \times \mathbb{H}_2)'']\otimes[\{|\psi>,\{0,1\}\} \in \mathbb{k}']$$

или

$$F: f''\circ f', f'=f,$$

където символът ⊗ обозначава операцията тензорно умножение (англ. tensor product) [46]. Съставната функция f′′, визуално изобразена на Фиг. 2.5, от своя страна има вида

$$f'': \{0,1\}^2 \in GF(2^2) \rightarrow \{|\psi>,\{0,1\}\} \in \mathbb{k}' \mid \{0,1\}^2 \in GF(2^2).$$

За съседни двубитови символи X_iX_{i+1}, принадлежащи на случайна двоична последователност, функцията f′′ характеризира следния преход

$$X_{i+1} \rightarrow (|\psi>_i,B_i) \mid X_i),$$

където символът ". | ." означава, че преходът зависи от стойността на X_i.

2.2.2. МЕТОД ЗА УВЕЛИЧАВАНЕ НА ЕФЕКТИВНОСТТА НА НИУ-КРКК МОДЕЛ.

С цел увеличаване на ефективността и дължината на крайния криптографски ключ s, се въвежда изложеният по-долу процес на *удължаване на ключовата последователност* (УКП, англ. key expanding), като се използва класическата информация Ψ_i.

Приемайки, че дадена двоична последователност s има елементи $s_i = \{0,1\} \in GF(2)$, които са напълно случайни ($H(s_i) = 1$) и поверителни ($I_E(s_i) = 0$), функцията K, характеризираща УКП, има вида

$$K: \{0,1\} \in GF(2) \rightarrow \{0,1\}^2 \in GF(2^2) \mid [\{0,1\}^2 \in GF(2^2), \{0,1\} \in GF(2)].$$

Този вид на функцията може да се представи символно по следния начин

$$s_i \rightarrow S_i \mid (\Psi_j,s_{i-1}); S_i \in \{0,1\}^2,$$

Тази функция се извършва само в случаите за (i)mod2 = 1, като i = 0,...,N-1. Трябва да се отбележи, че j = 0,...,(N/2)-1. Символът S_i обозначава резултата от функцията, докато $\Psi_j = \{0,1\}^2$ са спомагателните двубитови символи. С други думи, четните символи S_i (i = 0,2,4,...) са еднобитови, равни на съответните s_i, а нечетните S_i (i = 1,3,5,...) са двубитови. Функцията K се характеризира със следните таблица и визуално опредставяне. Нечетничте елементи S_i се обозначен допълнително чрез S^o_i.

Табл.2.2. Кодираща таблица за процеса УКП при i = 1,3,5,..., т.е. за нечетните символи $S_i(S^o_i)$.

S^o_i	s_i	s_{i-1}	Ψ_j	S^o_i	s_i	s_{i-1}	Ψ_j
00	0	0	00	01	0	0	01
01	0	1	00	00	0	1	01
10	1	0	00	11	1	0	01
11	1	1	00	10	1	1	01
10	0	0	11	11	0	0	10
11	0	1	11	10	0	1	10
00	1	0	11	01	1	0	10
01	1	1	11	00	1	1	10

Таблицата може математически да се представи чрез израза

$$S_i^o = \Psi_j \oplus s_i s_{i-1} \oplus A_j = (\Psi_j + s_i s_{i-1} + A_j) \bmod 2, \tag{2.1}$$

където

$$A_j = 0 \,||\, \Psi_j^1. \tag{2.2}$$

В този израз символът "||" обозначава операцията конкатенация (англ. concatenation) и Ψ^1_j идентифицира старшия бит на двубитовия символ Ψ_j.

2.3. АНАЛИЗ НА СИГУРНОСТТА НА МЕТОДИТЕ ЗА УВЕЛИЧАВАНЕ НА ЕФЕКТИВНОСТТА

В тази точка се извършва анализ на сигурността на процесите ККвК и УКП. За да бъдат тези процеси сигурни е необходимо да се докаже, че знанието на спомагателните битове, използвани при изпълнението им, не предоставя информация на НЛ. Количеството изтекла информация се оценява чрез понятието взаимна информация [72]

$$I(x;y) = H(x) - H(x|y), \tag{2.36}$$

където x и y са две различаващи се случайни променливи, H(.) е ентропия на случайна променлива и H(.|.) е условната ентропия на две променливи [46].

2.3.1. СИГУРНОСТ НА ККвК.

При анализа на сигурността на този метод квантовите системи се разглеждат по двойки (|Ψ>,[|ψ>,B)]), като за съставните им части се допуска следното:

(1) P(Ψ) = 0.25, P([ψ,B]) = 0.25 – данните, кодирани в квантовите системи Ψ и двойката [ψ,B] съответстват на случайни променливи, имащи равномерно вероятностни разпределения, т.е. H(Ψ) = 2,; H([ψ,B]) = 2.

(2) Състоянията на Ψ са напълно неизвестни за неоторизирани лица в комуникацията: I(Ψ;*) = 0, където * обозначава притежанието на каквато и да странична, допълнителна информация.

В тази точка се цели доказването на условието I(ψ;B) = 0, т.е. това, че спомагателните символи B не предоставят информация на неоторизирано лице (НЛ) за състоянията на ψ.

Преди да се докаже I(ψ;B) = 0 се показва недостатък на процеса ККвК и влиянието му върху сигурността на ККвК-ДККК протокола – какво количество информация изтича при прилагането на ККвК. Своевременно се представя и решение за това.

Недостатък:

Чрез Ψ се предават двубитови съобщения. Чрез двойката [ψ,B] също се предават двубитови съобщения. Стойността на двубитовото съобщение, пренасяно от [ψ,B], зависи от стойността на предхождащо го Ψ. Знаейки B, НЛ има сведения за това кои 8 от 16 възможни комбинации биха се изпратили с определена тройка (Ψ,ψ,B). Например, ако B = 0 възможните последователности са

|Φ+>|V>, |Φ+>|H>, |Φ->|V>, |Φ->|H>, |Ψ+>|V>, |Ψ+>|H>, |Ψ->|V>, |Ψ->|H>.

Тези двойки съответстват на 8 съобщения, т.е.

$$I(\psi;B)=H(\psi)-H(\psi|B)=1[\text{bit}]. \qquad (2.37)$$

Решение на недостатъка:

Чрез двуквантовите състояния |Ψ> (|Φ+>,|Φ->,|Ψ+>,|Ψ->) или чрез използване на предварително споделена конфиденциална двоична последователност може да се *замаскира* стойността на B. Например,

$$|\Phi+>, |\Psi+> \Rightarrow B' = B,$$

$$|\Phi->, |\Psi-> \Rightarrow B' = \neg B,$$

където символът “¬” идентифицира двоична инверсия. Замаскирването на B означава, че информацията на НЛ относо действителната стойност на B е $I_E(B')=0$, защото H(B´) приема стойност единица (H(B´)=1). Това е така само при условие, че $Pr(|\Psi_i>) = 0.25$ (или $Pr(C_i) = 0.5$ – за случая, когато се използва предварително споделена конфиденциална двоична последователност C_i). Следователно от гледна точка на НЛ всяка възможна стойност на двойката (Ψ,ψ) има вероятност да възникне, понеже НЛ не знае действителната стойност на B – тя е неопределена (H(B)=1). Тогава възможните стойности на (Ψ,ψ) от гледната точка на НЛ са:

$$|\Phi+>\otimes\{|V>,|H>,|D>,|A>\},\ |\Phi->\otimes\{|V>,|H>,|D>,|A>\},$$
$$|\Psi+>\otimes\{|V>,|H>,|D>,|A>\},\ |\Psi->\otimes\{|V>,|H>,|D>,|A>\}.$$

Сега се определя стойността на взаимната информация I(ψ;B) в случая на замаскирано B. Това се прави с цел да се потвърди факта, че не изтича информация до НЛ за пренасяното от квантовите системи съобщение. Използвайки допускането (1), както и израза (2.38) и резултата от него (2.42) за взаимната информация I(ψ;B) се получава

$$I(\psi;B)=H(\psi)-H(\psi|B)=2-2=0[\text{bits}]. \qquad (2.38)$$

По този начин се доказва, че ККвК е сигурен метод, такъв при който не изтича информация за състоянията на пренасяните квантови системи. Подходът със замаскирането стойността на B чрез стойността на Ψ е удачен само в случая, когато НЛ няма никаква информация за Ψ. В противен случай е нужно използването на предварително споделена конфиденциална двоична последователност за замаскирането на B.

2.3.2. СИГУРНОСТ НА УКП.

В тази точка се представя доказателство за валидността на условието $I(S_i;\Psi_j) = I(S;\Psi_j) = 0$ [bits], т.е. за това дали спомагателните символи Ψ_j предоставят информация за символите на крайния ключ S_i.

За доказването на това условие се правят следните допускания:

(1) Ψ_j (вж. т.2.2.2) са двубитови случайни променливи с равномерни вероятностни разпределения – $H(\Psi_j) = 2$;

(2) s_i (вж. т.2.2.2) са двоични случайни променливи с равномерни вероятностни разпределения и са напълно конфиденциални – $H(s_i) = 1$, $I(s_i;\Psi_j) = I(s_i;\Psi) = 0$, където Ψ е последователността, съставена от спомагателните символи Ψ_j.

(3) понеже четните символи на крайния ключ S_i (i = 0,2,4,...) приемат стойностите на s_i, то тогава $H(S_i) = 1$, $I(S_i;\Psi_i) = 0$ за i = 0,2,4,... .

На база на допусканията пред нас остава следната задача: да се докаже, че спомагателните символи Ψ_j не допринасят за изтичане на информация относно нечетните елементи на крайния ключ S_i (i = 1,3,5,...).

В последващата част на доказателството се използва следното обозначение: $S_j = S^o_i$.

Доказването на $I(S_j;\Psi_j) = I(S;\Psi_j) = 0$ започва с показването, че $H(S_j) = 2$. Това се извършва по следния начин. Тъй като S_j зависи от Ψ_j и $s_{i-1}s_i$, вероятността $Pr(S_j)$ може да се дефинира като $Pr(s_{i-1}s_i|\Psi_j)$, т.е. $Pr(S_j)=Pr(s_{i-1}s_i|\Psi_j)$. Тази вероятност се дефинира по следния начин [125]

$$\Pr(s_{i-1}s_i|\Psi_j)=\Pr(s_{i-1}s_i\cap\Psi_j)/\Pr(\Psi_j). \tag{2.46}$$

Понеже $s_{i-1}s_i$ и Ψ_j са независими променливи, $Pr(s_{i-1}s_i\cap\Psi_j)$ приема вида [125]

$$\Pr(s_{i-1}s_i\cap\Psi_j)=\Pr(s_{i-1}s_i)\Pr(\Psi_j). \tag{2.47}$$

Тогава по-горният израз се преобразува в

$$\Pr(s_{i-1}s_i|\Psi_j)=\Pr(s_{i-1}s_i)\Pr(\Psi_j)/\Pr(\Psi_j). \tag{2.48}$$

Ако се приеме, че $s_{i-1}s_i$ and Ψ_j са напълно случайни променливи, както е направено в началото на анализа, тогава $Pr(s_{i-1}s_i) = 0.25$ и $Pr(\Psi_j) = 0.25$. Следователно

$$\Pr(S_j)=\Pr(s_{i-1}s_i|\Psi_j)=(0.25\times0.25)/0.25=0.25. \tag{2.49}$$

По този начин математически се доказа, че S_j са случайни променливи.

От Табл.2.2 (вж. Глава II т. 2.2.2) се вижда, че всяка възможна стойност на Ψ_j отговаря на всички възможни стойности на S_j. Това означава, че $H(S_j|\Psi_j) = 2$, понеже $H(\Psi_j) = H(s_is_{i-1}) = 2$, както е прието в началото на анализа. С други думи, знаейки Ψ_j НЛ не може да предскаже стойността на S_j. Това математически се доказва по следния начин. Условната ентропия се изчислява както следва [126]

$$H(A|B)=\sum_b \Pr(B=b)H(A|B=b), \tag{2.50}$$

където

$$H(A|B=b)=-\sum_{a}\Pr(A=a|B=b)\log_2\Pr(A=a|B=b). \tag{2.51}$$

За случая на УКП, променливите A и B от горните изрази съответстват на S_j и Ψ_j, т.е. $A \equiv S_j$, $B \equiv \Psi_j$ ($S_j \in \{0,1\}^2$, $\Psi_j \in \{0,1\}^2$). Първо се изчисляват ентропиите $H(S_j|\Psi_j=\Psi)$, а след това и величините $H(S_j|\Psi_j)$. Понеже изчисляването на $H(S_j|\Psi_j=\Psi)$ е еднотипно за всички стойности Ψ на Ψ_j, в следващите редове се представя изчисляването само на $H(S_j|\Psi_j=00)$, като се използва изразът (2.22):

$$\begin{aligned}H(S_j|\Psi_j=00)=&-\Pr(S_j=00|\Psi_j=00)\log_2\Pr(S_j=00|\Psi_j=00)+\\&\Pr(S_j=01|\Psi_j=00)\log_2\Pr(S_j=01|\Psi_j=00)+\\&\Pr(S_j=10|\Psi_j=00)\log_2\Pr(S_j=10|\Psi_j=00)+\\&\Pr(S_j=11|\Psi_j=00)\log_2\Pr(S_j=11|\Psi_j=00).\end{aligned} \tag{2.52}$$

В този израз са налице вероятности, които са неизвестни до този момент – това са условните вероятности $\Pr(S_j=S|\Psi_j=\Psi)$. Стойностите на тези вероятности се определят както следва. Известно е, че S_j зависи от Ψ_j и $s_{i-1}s_i$. За всяко Ψ_j четирите стойности на $s_{i-1}s_i$ (00,01,10,11) е възможно да възникнат. Появата им е равновероятна - в началото на анализа е прието, че $H(s_{i-1}s_i) = 2$. Тези четири стойности на $s_{i-1}s_i$ съответстват на четири стойности на S_j = 00, 01, 10, 11. Това означава, че за дадена стойност на Ψ_j е възможно S_j = 00 или 01 или 10 или 11, като тези стойности са равновероятни.

Условната вероятност се изчислява по следния начин [125]

$$\Pr(A|B)=\Pr(A\cap B)/\Pr(B), \tag{2.53}$$

където $\Pr(A\cap B)$ е вероятността, съответстваща на случая когато и двете събития A=a и B=b възникват едновременно. Ако A и B са независими променливи, тогава [125]

$$\Pr(A\cap B)=\Pr(A)\Pr(B). \tag{2.54}$$

От Табл. 2.2 се вижда, че $\Pr(S_j\cap\Psi_j)=1/16=0.0625$ – S_j = S в една четвърт от случаите, когато Ψ_j = Ψ. Следователно,

$$\Pr(S_j|\Psi_j)=\Pr(S_j\cap\Psi_j)/\Pr(\Psi_j)=0.0625/0.25=0.25. \tag{2.55}$$

Забележете, че това важи за всички възможни стойности на S_j и Ψ_j. Заменяйки стойността от израз (2.24) за условните вероятности $\Pr(S_j=S|\Psi_j=\Psi)$ от израз (2.21), получаваме за ентропията $H(S_j|\Psi_j=00)$ стойността 2. Стойностите на останалите $H(S_j|\Psi_j)$ (за Ψ_j=01, Ψ_j=10 и

Ψ_j=11) също приемат тази стойност. Като резултат получаваме за условната ентропия от (2.19), при допуснато условие $H(\Psi_j) = 2$,

$$H(S_j|\Psi_j)=\sum_b \Pr(\Psi_j=\Psi)H(S_j|\Psi_j=\Psi)=4\times(0.25\times 2)=2. \quad (2.56)$$

Това води до следния резултат за взаимната информация $I(S_j;\Psi_j)$

$$I(S_j;\Psi_j)=H(S_j)-H(S_j|\Psi_j)=2-2=0[\text{bits}],\forall j. \quad (2.57)$$

Тъй като този израз важи за всяко j:

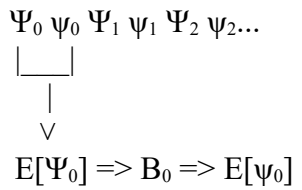
$$I(S_j;\Psi_j)\rightarrow I(S;\Psi)=0[\text{bits}]. \quad (2.58)$$

По този начин се доказва изискването за сигурност на процеса УКП.

2.3.3. ОНАГЛЕДЯВАНЕ НА СИГУРНОСТТА НА ККвК ЧРЕЗ ПРОГРАМНА РЕАЛИЗАЦИЯ НА ВЪЗМОЖНИ АТАКИ.

За допълнително доказване, че спомагателните битове не носят съществена информация за данните, пренасяни от едноквантови и двуквантови системи, са написани две програми на програмния език C++. В тази точка се използва обозначението **E[.]** - то означава догатване стойността на символ.

Написана е програма, представена в Приложение 3 и визуално онагледена на Фиг. 2.12, която има за цел да покаже, че при прилагане на ККвК със замаскирване НЛ се получава резултат, идентичен на този при тривиалното догатване: догатване на символите пренасяни от двуквантовите и едноквантовите системи при положение, че не се наблюдава класическия канал, т.е. не се вземат под внимание спомагателните символи. В този случай за всяка двуквантова система се догатва 1 от 4 възможни състояния, съответстващи на даннови символи. На теория това води до успех в 25% от опитите - това може да се отъждестви с ентропия: H(x) = 2.

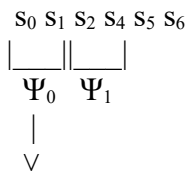


Фиг.2.12. Целева атака за придобиване на информация от изпълнението на процеса ККвК в случай на замаскирани спомагателни символи B.

Резултатът от програмата е следният. От 32768 даннови двубитови символа са отгатнати 8250 символа, т.е. ~1/4 от символите са отгатнати. Това означава, че НЛ не получава информация при изпълнението на атаката – НЛ има осреднена вероятност от близо 25% за да отгатне даден двубитов символ, пренасян от двуквантова или едноквантова система.

2.3.4. ОНАГЛЕДЯВАНЕ НА СИГУРНОСТТА НА УКП ЧРЕЗ ПРОГРАМНА РЕАЛИЗАЦИЯ НА ЦЕЛЕВА АТАКА.

За УКП също е разработена програма (вж. Приложение 4), с помощта на която да се покаже, че знанието на спомагателните символи за този процес (в този случай те са обозначени с Ψ_j) не води до по-голямо количество отгатнати символи в случай, че се проведе атака чрез догатване. При него първо се догатват първите два символа s_0 и s_1 на **УК** ключа, входната последователност за УКП алгоритъма. Вземайки под внимание първия спомагателен символ Ψ_0 се догатват първите два символа на **УКП** ключа (вж. т.2.2). В последствие се продължава по този начин, като се обхождат по двойки символите s, докато **УК** ключа привърши. Атаката, която се реализира чрез тази програма, е онагледена визуално на Фиг. 2.13.



$$(E[s_0],E[s_1],\Psi_0) \Rightarrow E[S_0],E[S_1];\ S_0 \in \{0,1\},\ S_1 \in \{0,1\}^2$$

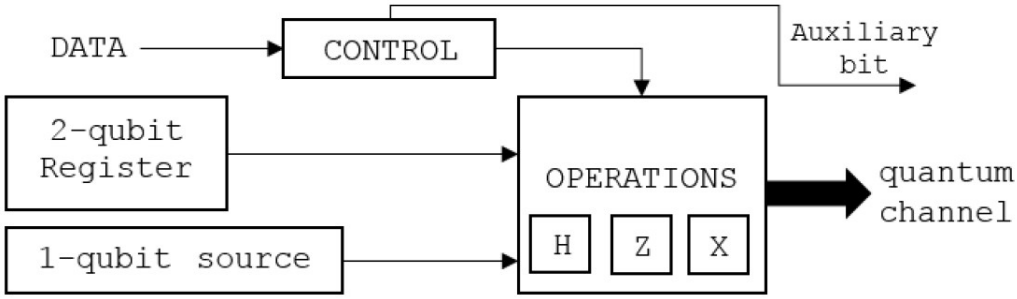
Фиг. 2.13. Целева атака за придобиване на информация от изпълнението на процеса УКП.

Резултатът от програмата е следния. От 24576 двоични символи на удължения ключ са отгатнати 8026. От тях 4012 бита са отгатнатите еднобитови символи на удължения ключ, отговарящи на четните символи на тази ключова последователност, а 4014 бита са тези, отгатнати от двубитовите символи на удължения ключ, отговарящи на нечетните символи. Това означава, че НЛ не получава информация за четните символи, както и за нечетните понеже НЛ отгатва ~1/2 от четните символи и ~1/4 от нечетните символи, т.е. ентропията H спрямо тези символи е максимална - за четните H = 1, за нечетните H = 2.

2.4. БЛОКОВА СХЕМА НА УСТРОЙСТВО ЗА ККвК.

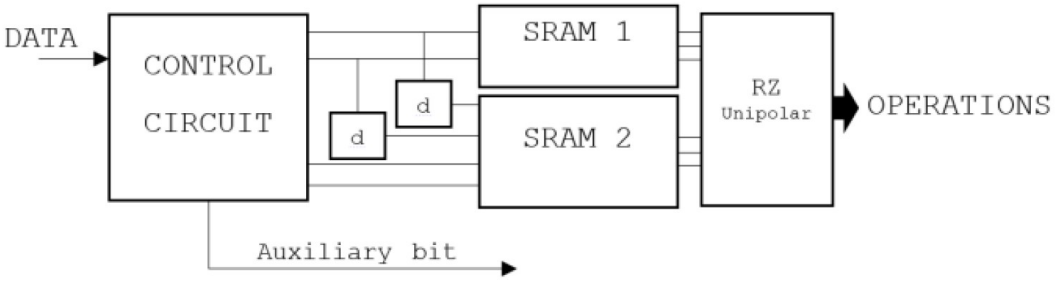
2.4.1. КОДИРАЩО УСТРОЙСТВО ЗА ККвК.

В тази точка се предлага схемно решение за кодиращо устройство, изпълняващо процеса ККвК. Това устройство се представя чрез блокова схема, показана на Фиг.2.14.



Фиг.2.14. Блокова схема на кодиращо устройство за ККвК метода.

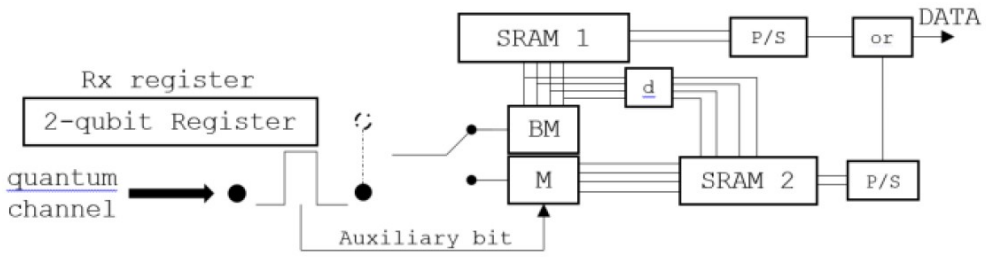
Кодерът се състои от три части: (i) фидер на квантови системи (2-QUBIT REGISTER, 1-QUBIT SOURCE), (ii) обработване на квантови системи (OPERATIONS) и (iii) управляваща част (CONTROL). При това схемно решение управляващата част е в основата на кодиращия процес. Тази част се характеризира със следната блокова схема.



Фиг.2.15. Блокова схема на УЧ за ККвК кодер. [d – delay (клетка памет – D тригер), SRAM – статична RAM, RZ (Return-to-Zero) Unipolar – RZ кодер за синхрон на потоците от SRAM модулите.]

2.4.2. ДЕКОДИРАЩО УСТРОЙСТВО ЗА ККвК.

В тази точка се предлага декодиращо устройство, което е в съответствие с кодирането, представено по-горе. Декодерът се характеризира с блоковата схема представена на Фиг.2.20.



Фиг.2.20. Блокова схема на ККвК декодер. [d – delay (клетка памет – D тригер), SRAM – статична RAM, P/S – паралелно-сериен преобразувател, or – логически елемент „ИЛИ“, BM – измерване на многофотонни (EPR двойки) системи, M – измерване на еднофотонни системи]

Това устройство може да се раздели на три основни, съставни части: (1) приемане и детектиране, (2) декодиране и (3) паралелно-серийно преобразуване. Декодирането се извършва в SRAM модулите.

ГЛАВА III. ПРИЛАГАНЕ НА МЕТОДИТЕ ЗА УВЕЛИЧАВАНЕ НА ЕФЕКТИВНОСТТА ПРИ ДККК И КРКК.

В тази глава се представят: (1) ДККК протокол, базиран на метода ККвК; (2) НИУ-КРКК протокол, базиран на метода УКП. Освен това се анализират ефективностите на тези протоколи, както и се извършва сравнение с техните класически алтернативи (ДККК [38] и НИУ-КРКК [9]).

3.3. ПРИЛАГАНЕ НА МЕТОД ККвК КЪМ ПРОТОКОЛ ОТ ТИПА ДККК.

Методът ККвК е процес за кодиране на информация върху квантови системи, както е представено в Глава II. Той е избран да се приложи към стандартния ДККК протокол [38] с цел подобряване общата ефективност на протокола. Прилагането изисква частично модифициране на някои от стъпките на ДККК модела, представен в т.3.2. Модифицираният протокол има следните стъпки.

1> Участникът A подготвя N на брой корелирани двойки в състоянието $|\Phi+\rangle$ (праволинеен базис) или $|\Phi+\rangle'$ (диагонален базис), където N є $2\mathbb{Z}_+$. Състоянията $|\Phi+\rangle$, $|\Phi+\rangle'$ се избират на случаен принцип.

2> От първите двунивови системи на корелираните двойки се сформира блок от N на брой квантови частици, наречен C-последователност (или I *трансферен блок*). Тази

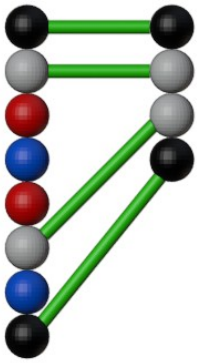
последователност се изпраща на участник B, който е получателят в комуникационния процес на протокола.

3> Участник B разделя този блок на две равни подгрупи – едната подгрупа се използва за проверка на проверка за наличие на НЛ (неоторизирано лице), а другата за предаване на M-последователността (II *трансферен блок*). Разделянето се извършва на случаен принцип. Освен това участник B избира на случаен принцип базисите, по отношение на които да бъдат измерени контролните системи, които съставят подгрупата за проверка на квантовия канал. Извършва се измерването на контролните системи. След това участник B съобщава по публичния класически канал позициите на контролните системи, базисите спрямо които са измерени системите и резултатите от измерванията.

4> Участник A измерва своите контролни системи, използвайки същите базиси като участник B. Тези контролни системи съответстват на позициите на контролните системи на участник B – контролните системи на A и B съставляват корелирани двойки. Участник A сравнява резултатите от своите измервания и резултатите от измерванията на участник B и определя вероятността за грешка (англ. error rate – ER) при тези измервания. Ако ER има малка стойност, намира се под предварително определена прагова стойност, участниците A и B продължават изпълнението на стъпките по протокола. В противен случай те прекратяват тази сесия и започват стъпките на протокола отначало.

5> След четирите стъпки, извършени досега, останаха N/2 наброй корелирани двойки – M-последователност. Половината от тях се използват за контролни при втория трансфер на квантови системи. Контролните системи се избират на случаен принцип и също на случаен принцип се обработват – на всяка една от тях на случаен принцип се прилага една от четирите операции I, X, Z, или iY [46]. Освен това участникът A генерира N/2 едноквантови системи – N/4 за пренос на данни и N/4 за проверка на квантовия канал. Данновите едноквантови системи, заедно с останалите N/4 на брой двуквантови системи, се подлагат на ККвК кодиране (вж. Глава II, т.2.2.1). Контролните едноквантови системи, подобно на двуквантовите, се подлагат на една от четирите операции I, X, Z, или iY, които се избират на случаен принцип. Данновите едноквантови системи се включват в M-последователността, като се спазва следната подредба: $\Psi_0\ \psi_0\ \Psi_1\ \psi_1$ ..., където Ψ_i са данновите двуквантови системи, а ψ_i са данновите едноквантови системи. Това означава, че едноквантовите системи се поставят между данновите двуквантовите системи, както е представено с пример на Фиг.3.4. Позиционирането на

контролните едноквантови системи не е от значение – поставят се на случаен принцип в М-последователността. След подреждането на М-последователността, тя се изпраща на участник В.



Фиг. 3.4. Подредба на контролни и даннови квантови системи във II трасферен блок (лявата колона). Дясната колона изобразява квантовите системи останали от I трансферен блок. В тази фигура се използват следните цветови означения: черни системи – двуквантови контролни системи, червени системи – едноквантови контролни системи, бели системи – двуквантови даннови системи, сини системи – едноквантови даннови системи. Със зелени линии се отбелязват двуквантовите системи, т.е. свързани са корелирани двойки квантови системи.

6> Участник В приема М-последователността. Участник А съобщава позициите на контролните системи в тази последователност, както и операциите извършени върху тях. Участник В измерва контролните корелирани двойки и определя вероятността за грешка ER. На база на стойността на ER, участникът В взема решение за това дали да се спре изпълнението на протокола или да се продължи. Ако стойността на ER е приемлива, участник А изпраща спомагателните битове B_i, които се използват от участник В за извършване на ККвК декодиране.

7> Участникът В извършва ККвК декодиране съгласно принципите, изложени в Глава II, т.2.2.1.

8> Участниците А и В изпълняват алгоритъм за корекция на грешки **КГ** [71].

9> Участниците А и В изпълняват алгоритъм за повишаване на конфиденциалността УК [70].

3.4. ПРИЛАГАНЕ НА МЕТОДА УКП КЪМ ПРОТОКОЛА НИУ-КРКК.

Методът УКП е процес, който удължава крайния, конфиденциален ключ на КРКК протокол. Той е избран да се приложи към НИУ-КРКК протокола с цел да се увеличи ефективността му. Прилагането на процеса УКП води до една единствена промяна в НИУ-КРКК протокола. Тази промяна е въвеждането на допълнителна стъпка в края на всяка протоколна процедура – изпълняване на УКП. Всички характерни стъпки за НИУ-КРКК (вж. т.3.1) не се променят. Следователно за протокол УКП-НИУ-КРКК имаме следните протоколни стъпки:

1> ÷ **9>** са същите като тези описани в т.3.1.

10> На базата на получените в стъпка **4>** данни ψ_i (ψ_i=0 ако резултатът от БС измерването е $|\Psi+>$; ψ_i=1 ако резултатът е $|\Psi->$), участниците А и В изпълняват процеса УКП, описан в Глава II, т.2.3, за получените валидни резултати от БС измерването в междинната точка на комуникационната система.

3.5. ОЦЕНЯВАНЕ НА ЕФЕКТИВНОСТТА.

В настоящата работа се предлага за оценка на ефективността да се използва следния израз, който е следствие на израза (3.2):

$$E = b_s/(n+N), \tag{3.3}$$

където b_s – брой на предадените двоични еднобитови символи, n – общият брой на използвани квантови двунивови системи, N – брой на използваните битове в протокола.

$$\Delta t = M/R, \tag{3.5}$$

където M [bit, брой квантови системи] е броят на битовете или двунивовите квантови системи, които се пренасят при изпълнението на протокол, а R [bit/s или кв. с-ми/s] е скоростта, т.е. броят на битовете или квантовите системи, пренасяни за единица време през дадена точка от комуникационната система. Приема се, че скоростта е една и съща по цялата комуникационна система. По дефиниция е известно, че M = n + N. Като се знае от (3.3), че (n + N) се равнява на (b_s/E), за връзката между комуникационната продължителност и ефективността се получава следното

$$\Delta t = M/R = (1/R)(b_s/E) = b_s/E \cdot R. \quad (3.6)$$

3.5.1. ОЦЕНЯВАНЕ НА ЕФЕКТИВНОСТТА НА ККвК-ДККК.

За да се оцени подобрението, което ККвК внася в ДККК протокол, първо се определя ефективността на стандартния ДККК модел. Базирайки се на протоколното описание в т.3.2, стандартният ДККК модел се характеризира с ефективност

$$E = 1/10. \quad (3.7)$$

На базата на предложения в т.3.3 протокол за ККвК-ДККК се изчислява ефективност

$$E' = 1/7. \quad (3.9)$$

За сравнение на ефективностите на двата протокола ККвК-ДККК и ДККК се дефинира следното отношение

$$\Delta = E'/E. \quad (3.10)$$

Този параметър, наречен тук *подобрение*, показва с колко пъти ККвК-ДККК е по-ефективен от стандартния протокол. Въз основа на гореполучените стойности на ефективността за ККвК-ДККК и ДККК за параметъра Δ се получава

$$\Delta = (1/7)/(1/10) = 10/7 = 1.428. \quad (3.11)$$

3.5.2. ОЦЕНЯВАНЕ НА ЕФЕКТИВНОСТТА НА УКП-НИУ-КРКК.

При оценяването на ефективността на НИУ-КРКК протокола се приема, че квантовият канал е без шумове. Следователно се пренебрегват процедурите **КГ** и **УК** (вж. Глава III т.3.1), понеже детектирането на грешки в установения **ОК** криптографски ключ директно осведомява за присъствието на НЛ.

За да се оцени подобрението, което УКП внася в НИУ-КРКК протокол, първо се определя ефективността на стандартния НИУ-КРКК модел. Базирайки се на протоколното описание в т.3.4, стандартният НИУ-КРКК модел се характеризира с ефективност

$$E = 0.026 . \quad (3.14)$$

При варианта УКП-НИУ-КРКК на този протокол се извършва допълнителна операция върху крайния ключ, чрез която се постига ефективност

$$E' \approx 0.0395 . \quad (3.15)$$

Следователно прилагането на УКП води до подобрение на ефективността с (вж. Формула (3.10))

$$\Delta = E'/E = 0.0395/0.026 = 1.52 \approx 1.5 . \quad (3.16)$$

ГЛАВА IV. ОЦЕНЯВАНЕ НА СИГУРНОСТТА И ПРАКТИЧНОСТТА НА ККвК-ДККК И УКП-НИУ-КРКК ПРОТОКОЛИТЕ. ПРЕДСТАВЯНЕ НА МЕТОД ЗА ОБОБЩЕНА ОЦЕНКА.

В тази глава се представя метод за обобщена за оценка на КМПКК модели, който включва оценяване на ефективността, сигурността и практичността. За тази цел се дефинират оценките за сигурност и практичност и се заема оценката за ефективност, предложена в [24].

4.1. МЕТОД ЗА ОБОБЩЕНА ОЦЕНКА.

В опит да се оцени успехът на даден КМПКК (КРКК или ДККК/КПККК) модел, ние трябва да си зададем три въпроса: (1) Сигурен ли е протоколът?, (2) Ефективен ли е протоколът? и (3) Протоколът обуславя ли се с практична експериментална постановка?. Така, че само в случая, когато положителни отговори на тези три въпроса са дадени, ние можем да считаме, че даден модел е задоволителен, оптимален.

Отговори на трите въпроса се дават чрез трите параметъра: *ефективност*, която се оценява чрез количеството ресурси, включващи квантови системи и битове, използвани за трансфера на определено количество двоични символи; *сигурност*, която се оценява чрез степента на уязвимост към съществуващи атаки или чрез вероятността за детектиране присъствието на неоторизирани страни в комуникационния процес; и *практичност*, която се оценява чрез сложността на даден модел и устройствата, участващи при неговата реализация.

4.1.1. ОЦЕНКА НА СИГУРНОСТТА.

Общата оценка на сигурността на КМПКК модел се дефинира като комбинация от два параметъра: (i) *устойчивост на класическия канал* χ, която се определя чрез

$$\chi = H_e^{'} / H_e, \tag{4.21}$$

където H_e' е ентропията, когато неоторизираното лице наблюдава класическия канал, докато H_e е ентропията, когато лицето не наблюдава канала; (ii) *сигурност на квантовия канал* λ, която се определя чрез

$$\lambda = \min\left(ER_k\right), [\%] \tag{4.22}$$

където индексът k отчита броят на квантовите атаки, които се вземат под внимание в анализа, а ER вероятността за грешка, която се очаква дадена атака да породи.

Тогава общата оцценка за сигурността се определя чрез

$$\Sigma = (\chi + \lambda)/2. \tag{4.23}$$

Избрана е средноаритметична сума на параметрите χ и λ поради факта, че и двата са от голямо и еднакво значение за стойността на общата сигурност. Затова тегловните коефициенти пред χ и λ (нека ги обозначим съответно с j и k) в сумата са равни: j = k = 1/2.

4.1.2. ОЦЕНКА НА ПРАКТИЧНОСТТА.

Оценката на практичността на КМПКК протокол е следната. Тя се състои в определянето на това дали даден протокол отговаря на критериите:

- Използване на нелинейни оптични устройства, които имат ниска ефективност на работа. **(c_1)**
- Използване на повече от един тип квантов канал, което е равносилно на използване на повече от едно състояние на квантовия канал. Пример за това е случаят, когато се използват както двунивови квантови системи, така и корелирани квантови системи за

квантов канал. Такъв тип протокол изисква използването на два оптични източника . Друг пример е случаят, когато се използват два типа квантови канали, които се различават по даден тип квантова операция – изключение прави операцията H (англ. Hadamard gate) [46], която се използва за пренос на една квантова система от един базис в друг. **(c_2)**

- Използване на допълнителни класически операции, които изискват внедряването на конкретни класически устройства или осложняването на съществуващи такива. Пример за това е процес на кодиране или криптиране. Както е известно, тези процеси изискват използването на специални устройства за реализацията им, чиито присъствие води до намаляване на практичността на протокола. **(c_3)**

Гореизложените критерии могат да се представят чрез двоичен вектор. Понеже са въведени само три критерия, векторът се състои от следните три елемента

$$\mathbf{c} = c_i = [c_1\ c_2\ c_3],$$

където индексът i приема стойности от 1 до 3 (само цели числа). При това двоично представяне, c_i приема стойност ‚0‘ ако даден протокол отговаря на съответния критерий и ‚1‘ ако протоколът не отговаря на него. Използвайки предложения подход, базиран на критерии, практичността математически се дефинира чрез израза

$$\xi = \sum_i (1/n) c_i . \tag{4.24}$$

От горната формула ясно се вижда, че възможните стойности, които практичността може да приеме, са в интервала [0,1], т.е. $\xi \in [0,1]$.

4.1.3. ОЦЕНКА НА ОПТИМАЛНОСТТА.

Всяка комуникационна система, в която се използва ККК, има нужда от обобщена оценка относно ефективността, сигурността и практичността. Обобщеният критерии, който приемаме за тази оценка, се нарича оптималност. Въвеждайки оценка на оптималността направените анализи за КМПКК създават предпоставки за по-точно сравнение на съществуващите модели. Оптималността включва ефективността E, сигурността Σ и практичността ξ на КМПКК модел. Тя се дефинира чрез израза

$$\zeta = (E + \Sigma + \xi)/3. \tag{4.25}$$

Този параметър е представен като средноаритметичната сума на трите основни параметри на КМПКК. Понеже E ϵ [0,1], Σ ϵ [0,1], ξ ϵ [0,1], възможните стойности на оптималността също се намират в интервала [0,1].

ОБЩИ ИЗВОДИ И ЗАКЛЮЧЕНИЕ

В дисертационния труд се изследват и анализират възможностите за подобряване и оптимизиране на квантови модели за пренос на криптографски ключове (КМПКК): - определят се основните параметри, характеризиращи тези модели; - анализира се настоящото състояние на един от тях - ефективността; - анализират се подходите за сравнение и оценка на моделите.

На база гореизложените анализи в дисертационния труд се предлагат следните методи и методика за подобряване нивото на съществуващите квантови модели за пренос на криптографски ключове:

- Предлага се метод за увеличаване ефективността при пренос на данни посредством квантови системи за нуждите на КМПКК от тип ДККК. Той допринася за намаляване на общия брой на квантови системи и битове, които се използват за установяване на криптографски ключ с конкретна дължина. Това намаляване на ресурсите е за сметка усложняване на практическата реализация комуникационната система – нужно е използването на допълнителен източник на квантови системи или такъв с двойно по-високо бързодействие;
- Предлага се метод за увеличаване ефективността при установяване на крайни криптографски ключове за нуждите на КМПКК от тип НИУ-КРКК. Той допринася за двойно удължаване на размера на крайния криптографски ключ при отсъствие използването на допълнителни класически или квантови ресурси. Това удължаване на криптографския ключ е за сметка усложняване на комуникационните терминали, използвани в КМПКК системите – необходимо е въвеждането на допълнителни устройства или интегрирането на допълнителна операция в съществуващите устройства;

Методите са изградени с цел подобряване бързодействието на комуникациония процес, влизащ в състава на съответния модел.

- Предлага се метод за обобщена оценка на КМПКК модели.

Методиката се представя с цел по-коректно сравнение и оценка на съществуващи и бъдещи КМПКК модели.

ОСНОВНИ ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

Основните приноси в дисертационния труд, които могат да се изтъкнат, са следните:

1. Предложен е метод за увеличаване ефективността на ДККК моделите, наречен компресия на квантовия канал (ККвК).

2. Предложен е метод за увеличаване ефективността на НИУ-КРКК моделите, наречен удължаване на ключовата последователност (УКП).

3. Предложени са схемни решения на устройства (кодер и декодер), изпълняващи ККвК. Тези устройства са предназначени за идеален случай на комуникация – квантов канал без загуби.

4. Предложени са изрази за по-обобщено оценяване на ефективността и комуникационната продължителност на КМПКК моделите.

5. Предложен е модифициран протокол за ДККК комуникация, която се базира на ККвК. Извършен е анализ на ефективността, който показва, че прилагането на ККвК води до подобрение от 1.428 пъти спрямо стандартния ДККК модел.

6. Предложен е модифициран протокол за НИУ-КРКК комуникация, която се базира на УКП. Извършен е анализ на ефективността, който показва, че прилагането на УКП води до подобрение от 1.5 пъти спрямо стандартния НИУ-КРКК модел.

7. Предложен е метод за обобщена оценка на съществуващи модели за установяване на криптографски ключове по квантов път. Тази оценка е функция на ефективността, сигурността и практичността на моделите. Методът дава възможност за по-точно сравнение и оценяване на съществуващи и бъдещи модели за КМПКК.

ПУБЛИКАЦИОННА ДЕЙНОСТ

[П1] G. Bebrov, R. Dimova and E.Pencheva, Quantum Approach to the Information Privacy in Smart Grid, OPTIM-ACEMP Conference Proceedings, Brasow, Romania, 2017.

[П2] G. Bebrov and R. Dimova, Quantum Secure Communication Models Comparison, Annual Journal of Technical University of Varna, Vol.1, Issue 1, 2017.

[П3] G. Bebrov and R. Dimova, Efficient quantum secure communication using quantum channel compression, International Journal of Theoretical Physics, Vol**.** 59, 426-435, 2020.

[П4] G. Bebrov and R. Dimova, Teleportation-based quantum secure communication using quantum channel compression, Vol. 74, 33, 2020.

[П5] G. Bebrov, Efficient teleportation-based quantum secure communication using quantum channel compression, Vol. 74, 47, 2020.

[П6] G. Bebrov, P. Stoyanov and R. Dimova, Proposal of Encoder and Decoder for Quantum Channel Compression, BIA Conference, Varna, 2019.

[П7] G. Bebrov and R. Dimova, Proposal of Optimality Evaluation for Quantum Secure Communication Protocols by Taking the Average of the Main Protocol Parameters: Efficiency, Security and Practicality, World Academy of Science, Engineering and Technology International Journal of Physical and Mathematical Sciences Vol.13, No.2, 2019.

УЧАСТИЕ В НАУЧНОИЗСЛЕДОВАТЕЛСКИ ПРОЕКТИ ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯ ТРУД

1. ДН07/10 - „Изследване на архитектури, модели и методи за автономен мениджмънт в интернет на бъдещето“, р-л: проф. д.т.н. инж. Евелина Пенчева, ТУ-София, 2016г.
2. ПД1 - „Моделиране и изследване на квантови методи за запазване конфиденциалността на информацията“, р-л: проф. д-р инж. Розалина Димова, ТУ-Варна, 2018г.

ABSTRACT

The thesis is concerned with quantum key distribution models. It presents solution to the efficiency problem of these models. Two methods, which improve the efficiencies of certain quantum key distribution models (quantum secure direct communication – QSDC, and measurement-device-independent quantum key distribution – MDI-QKD), are introduced. One of the methods, called quantum channel compression – QCC, is an encoding procedure being different than the standard one. The other method, called key expanding - KE, is a procedure of increasing the length of the final (established) key in a quantum key distribution protocol. The thesis also presents a general method of evaluating the existing quantum key distribution models (protocols). This work is organized in four chapters as follows.

In Chapter 1, an analysis of the current state of quantum key distribution (QKD) models is set out. A classification of the different quantum key distribution models is made. The efficiency problem of these models is exposed. Also, this chapter emphasizes on the problem of lacking a general evaluation of the QKD schemes.

In Chapter 2, solutions to the efficiency problem of QSDC and MDI-QKD models are mathematically introduced, namely QCC and KE, respectively. Security analyses of these methods are presented by both mathematics and way of simulation.

Chapter 3 introduces novel QCC- and KE-based quantum secure communication protocols. The QCC-based protocol is an enhancement of a standard QSDC protocol, whereas the KE-based protocol is an enhancement of a MDI-QKD protocol. Moreover, efficiency analyses of these novel protocols are worked out.

Chapter 4 presents a general evaluation, called herein optimality, of quantum key distribution models. It is defined as a function of the main parameters of QKD: efficiency, security, and practicality. By way of example is shown the application of this general evaluation.