American Journal of Engineering Research (AJER) **2026**
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-15, Issue-4, pp-36-45
www.ajer.org
Research Paper Open Access

Attack strategies for quantum key distribution protocols

Tofig M. Mansurov[1]*, Nurali A. Yusifbayli[1], Elnur T. Mansurov[2]
[1]*Doctor of Technical Sciences, Professor*
[2]*Doctoral student*
[1,2]Azerbaijan Technical University, Department of Radio Engineering and Telecommunications
Corresponding Author: Tofig Mansurov

ABSTRACT : *This work is a study of three types of quantum key exchange protocols with qudit transfer, that is, prepare-and-measureprotocols using d+1 and two mutually nondisplaced bases and protocols with mixed qudits. The study is performed synchronously by several criteria, such as the protocol information security and the resistance of protocols to noncoherent attacks and to the photon number splitting attack, which is needed for determining the optimal type of protocols. In addition, the work provides the first ever analysis of the photon number splitting attack against the six-state protocol classified as a protocol with d+1 bases. It is concluded that prepare-and-measureprotocols with two bases are the optimal protocols in terms of information capacity and resistance to noncoherent attacks and to the photon number splitting attack.*

KEYWORDS : *resistance, information capacity, quantum protocol, quantum system, key distribution, qudit, photon, noncoherent attack*

Date of Submission: 03-04-2026 Date of acceptance: 14-04-2026

I. INTRODUCTION

One of the main issues in symmetric secret key cryptography is the development of procedures for the key exchange between the users of a communication path (subjects *A* and *B*). Currently, the secret key exchange is ensured by broadly using public-key schemes, for example, Digital Envelope Scheme or Diffie-Hellmann Key Exchange Algorithm [1]. These schemes boast only with computational strength, that is, use the finiteness of the computational capacities of the intruder (subject *E*). The alternatives to these key exchange schemes based on assymetrical cryptography are quantum key exchange systems the resistance of which is based on quantum physics laws and achieves theoretical information levels in certain conditions [2]. The main idea behind quantum key exchange is that, when the intruder manipulates quantum information carriers, it is highly probable that he distorts their states, which is detected by legitimate users. Thus the intruder cannot conduct an efficient interception unnoticed.

II. LITERATURE REVIEW

The theoretical information strength of quantum key exchange protocols (QKEP) requires estimating the amount of information that could have been captured by the intruder while implementing the protocol [2,14,15]. The QKEP stack consists from the protocol of the primary quantum path transfer; protocol of correcting errors in the strings resulting from the transfer; protocol of estimating the data leak of the intruder; secrecy strengthening protocol and resulting key generation protocol. The data leak to the intruder occurs in the first two phases of the stack. The complete consideration of all of the factors influencing the leak is an extremely complex task and has partially been executed so far only for several elementary protocols, for example, protocol BB84 [10]. This is why, only the information captured by subject E during the execution of the quantum transfer protocol is usually considered as tentative estimate. The respective quantitative characteristic is the highest of the two values: mutual information $I_{AE}(D)$ between Shannon subjects A and E or mutual information $I_{BE}(D)$ between subjects B and E that are functions of level D of errors made by the eavesdropping of subject *E*. For the attacks considered in this work $I_{AE}(D)=I_{BE}(D)$, which is why we shall further use $I_{AE}(D)$. Note that this quantity is only the bottom leak limit but an additional analysis of the leak while correcting errors for protocol BB84 extends this limit only by several percent [10]. Thus function $I_{AE}(D)$ can be considered an acceptable strength characteristic of any QKEP [1-3,5,7,10,19].

Another main characteristic of QKEP is information capacity; it shows the amount of information usable for generating a secret key during the transfer along a communication path of a quantum system. One of the ways of increasing information capacity is to replace cubits with multilevel quantum systems known as

qudits (quantum dits). Each qudit allows transferring $\log_2 d$ bits of classic information, where d is the dimension of the qudit's Hilbert space. It is obvious that the information capacity of the protocol increases with an increase in d; however, large-dimension quantum systems are still unusable for transfers because of difficulties with designing necessary equipment.

The information capacity of a protocol depends not only on the dimension of qudits in use but also on the scheme of the protocol itself. This work considers the protocol information capacity in ideal conditions, that is, ignores such influences as losses in the quantum path, eavesdropping-induced errors, and reduction in the length of the generated key after strengthening the secrecy because all of these factors depend on the specific conditions of implementing the protocol, not on the protocol scheme. Information capacity will be measured in bits per transferred qudit.

The QKEP with finite-dimension quantum systems, suggested to date, are divided in two types.

The first type is based on transferring single quantum states referred to nonorthogonal bases (this type of protocols is called prepare-and-measure protocols) [4-6]. The second type is based on distributing mixed quantum states among users [7]. Both types of protocols have already been tested for resistance to certain kinds of attacks. Thus, for example, dependences $I_{AE}(D)$ have been calculated for the intercept-resend qudit attack [1,16,17,20,23] and for the optimal noncoherent attack [3,5,7]). The resistance of protocol BB84 to the so called photon number splitting attack (PNS attack*)* has also been tested. The PNS attack is possible as a consequence of imperfections in the equipment currently in use in quantum cryptography [11,13]. There was also a comparative test of QKEP with qudits against the criteria of strength and information capacity [12]. However, in [12], the protocol resistance test was confined to the attacks possible only when the source of signals irradiated a qudit.

III. THE PURPOSE AND METHODOLOGY OF THE STUDY

The purpose of this study is to analyze the information parameters of qudits for the case of an attack with splitting the number of photons, as well as the stability of the protocol of its operation with six states.

The research methodology is a systematic analysis of the functioning of qudits based on the modeling and evaluation of the parameters of the processes of its functioning.

IV. MAIN STRATEGIES OF ATTACKS AGAINST QUANTUM KEY EXCHANGE PROTOCOLS

First, consider the attack of the intruder in case when the source of signals irradiates one qudit. In this case, attacks are divided in two classes [8,21,22].

The first class is noncoherent attacks. In these attacks, the intruder processes each qudit of subject A as separate. The easiest variant is the qudit intercept-resend attack referred to hereafter as the *IR*-attack. The intruder intercepts the qudits of subject *A*, measures their states in one of the bases used by the legitimate users, and then shares new qudits prepared in the measured states with subject *B*. Since the intruder does not pass the qudits of subject *A* along the quantum path but irradiates new qudits, this eavesdropping strategy is also known as nontransparent.

A more complex noncoherent attack is the mixing of auxiliary quantum systems (samples) of the intruder with qudits transferred along the channel (Fig. 1).

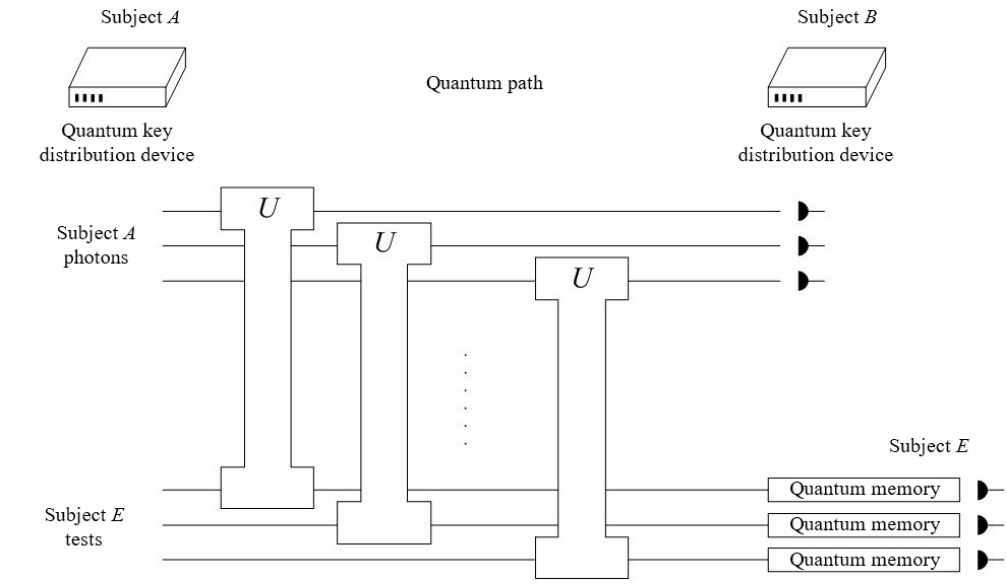


Fig. 1. Semitransparent noncoherent attack against a quantum key exchange protocol

In this case, each qudit of subject *A* is mixed with a separate sample independently from others and the qudits that have interacted with the samples are shared with subject *B*. Then the intruder keeps the samples in quantum memory and measures their states separately after the public message exchange among the legitimate users in the key screening phase is finished. The eavesdropping of public messages allows the intruder to know the basis used by subject *A* for each qudit and thus choose optimal measurement procedures for his samples so as to know more information. Of course, the states of the subject *A* qudits, with which the intruder mixes his samples, change after the mixing; however, in some cases, the level of errors made by the intruder in this attack can be weaker than in the nontransparent attack. This attack is also known as medium-transparent.

It should be noted that at any noncoherent attack the intruder can reduce the level of committed errors by reducing the amount of information obtained - for this purpose, he must intercept or mix with his samples only some of the resent qudits.

The second class encompasses so called coherent attacks (Fig. 2). In these attacks, the intruder can use any (unitary) method to mix a sample of any size with a whole group of transferred single qudits [8].

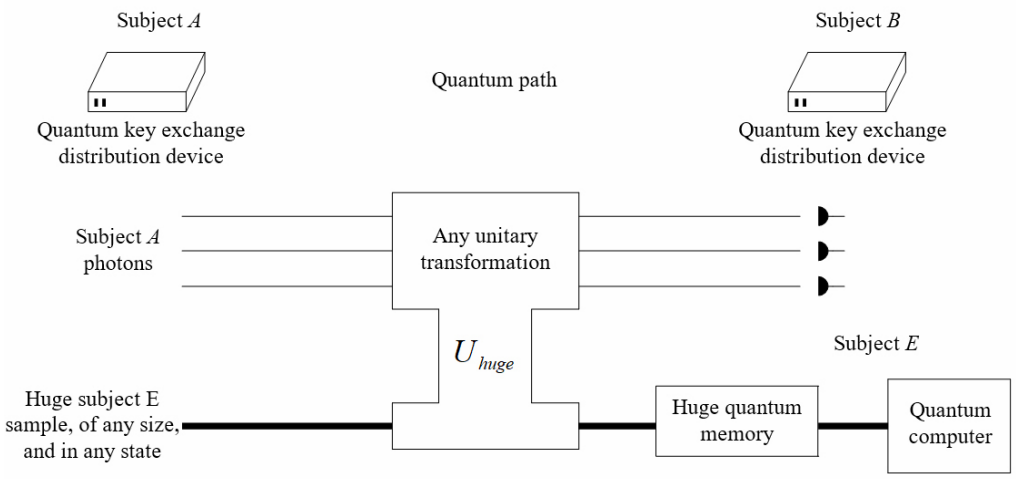


Fig. 2. Coherent attack against a quantum key exchange protocol

Then he keeps his big sample, until all of the public communication paths among the legitimate users are exhausted, and takes the most general measurement of the sample at his discretion. Note that, to make these attacks, the intruder must not only have a large quantum memory but also a multiqubit quantum computer (yet to be created); in other words, coherent attacks are currently technically impossible.

The photon number splitting attack is possible only on condition that the source irradiates more than one photon in one and the same state. These sources of signals are currently in use in quantum cryptography because single-photon sources have not been created yet. Modern quantum key exchange systems use weak coherent pulses irradiated by laser light-emitting diodes. The number of photons per pulse is determined by the Poisson distribution, that is, some of the transmitted pulses contain two or more photons.

To make a photon number splitting attack for each pulse, sent by subject *A*, the intruder must make a quantum nondestructive measurement of the number of photons in the pulse without influencing their polarization. Note that at the moment this measurement is very hard to make but technically possible. If the intruder sees more than one photon in the pulse, he withdraws a photon while letting the others reach subject *B* without impediment. Then the intruder mixes the intercepted photon with his sample and waits until the legitimate parties declare used bases after the transfer. Then, the intruder obtains the exact value of a transferred bit while measuring the state of the sample but without introducing any errors in the screened key; in other words, the attack remains undetected.

If the pulse carries one photon, the intruder can use various strategies. For example, he can simply let pass all single-photon pulses, which will allow the attack of the intruder to remain unseen. However, at a small average number of photons per pulse (in practice, the number of photons to which the equipment is adjusted is somewhere around 0.1) the number of multiphoton pulses will also be small, which will not allow the intruder to learn any significant information about the key. Another possible strategy of the intruder is a noncoherent attack against single-photon pulses. In this case, the intruder naturally introduces errors into the screened key. The number of such errors depends on the type of attack and on the fraction of single-photon pulses during the key transfer.

Another strategy of the intruder consists in blocking a part of single-photon pulses; as a result, subject *B* receives an empty pulse, that is, the gage does not register the photon. This blocking of some single-photon pulses allows the intruder to increase the fraction of multiphoton pulses, which allows him to increase the

amount of information about the key at the same level of errors introduced in the screened key. Since the modern gages used in commercial quantum key exchange systems have a low sensitivity and register only 20-30% of single photons on average and there are also losses of photons in the communication path, the intruder can therefore theoretically hide his attack. However, knowing the probability of obtaining an empty pulse with the available equipment, subject *B* can detect that the actual number of empty pulses significantly exceeds the expected number of these pulses. Note that subject *B* can also not only determine the number of empty pulses but also control the entire statistics about received signals while making a nondestructive measurement of the number of photons per pulse. In this case, the intruder will have to withdraw a photon only from a small part of multiphoton pulses while letting the other photons pass without obtaining any information.

The photon number splitting attack can be improved as follows: the intruder secretly replaces a quantum path between legitimate users with losses among them with an ideal path without losses or with much fewer losses [11]. In this case, the intruder will be able to block a certain part of single-photon pulses, while misrepresenting these losses as natural; in other words, the number of empty pulses received by subject B will be roughly the same as before the path's replacement. It is obvious that, for the original path with large losses, the intruder will be able to obtain almost the whole key and remain unnoticed. In addition, if the losses in the original path are very significant, the intruder can replace this path with a much more efficient path while preserving not only the fraction of emoty pulses expected by subject B but also the entire statistics about the number of photons per pulse. Note that, of course, it is very hard to replace an existing quantum path with a better path in practice.

The full theoretical analysis of the photon number splitting attack has been made so far only for protocol BB84. In this article this analysis has been made for the first time ever for the six-state protocol. In addition, the full theoretical analysis of QKEP for resistance against the coherent attack has been made so far only for protocol BB84 and for the six-state protocol [2,3,24]. In this article, the coherent attack against protocols with qudits is not considered.

V. RESISTANCE TO NONCOHERENT PREPARE-AND-MEASURE ATTACKS AGAINST PROTOCOLS WITH QUDITS

First of all, we shall consider an elementary IR attack against prepare-and-measure protocols with qudit transfer; this attack is a generalization for the multidimensional systems of protocol BB84 and the six-state protocol [2]. In these protocols, secrecy is ensured using at least two mutually nondisplaced bases like in protocol BB84. Two bases are designated as mutually nondisplaced (additional) on condition that any two basic vectors of these bases meet ratio $\langle i | j' \rangle = 1/\sqrt{d}$, where i is the base vector of the first basis, *j'* is the base vector of the second basis, and *d* is the size of the Hilbert space.

It is known that, if d is the degree of a prime number, there are exactly $d+1$ mutually nondisplaced bases in the $d-$ dimensional Hilbert space. Therefore, the maximal number of bases which can be used by legitimate users is $d+1$. For example, there are three such bases for the Hilbert space. The respective protocol using qubits and three mutually perpendicular nondisplaced bases is called the six-state protocol. Compared with protocol BB84, this protocol shows a somewhat better resistance to both, noncoherent and coherent attacks but is far less efficient ($1/3$ bit/qubit for the six-state protocol against $1/2$ bit/qubit for BB84) [11].

The mutual information between subjects *A* and *B* as the function of error level *D* of subject *B* is determined for protocols with qudits as in [3]:

$$I_{AB}(D) = \log_2 d + (1-D)\log_2(1-D) + D\log_2(D/2), \quad (1)$$

where bit is the information measurement unit like in the subsequent formulae for mutual information.

IR was analyzed in (6) for using both, two and $d+1$ mutually nondisplaced bases. In these cases, the expressions for the mutual information between subject *A* and the intruder are

$$I^{(2)}_{AE-IR}(D) = 2D/(1-1/d)\cdot\frac{\log_2 d}{2}, \quad (2)$$

$$I^{(d+1)}_{AE-IR}(D) = D/\left[1-1/(1+\mathrm{d})\cdot(1-1/d)\right]\cdot\log_2 d/(1-1/1+d)]. \quad (3)$$

The maximal error levels in legitimate users in case of the *IR* attack for two and $d+1$ bases determined by respective expressions $D^{(2)}_{IR\max} = (1-1/d)/2$ and $D^{(d+1)}_{IR\max} = [1-1/(1+d)(1-1/\mathrm{d})]$ are represented in Table 1.

Table 1. Maximal error levels in case of the *IR* attack

Hilbert qudit space dimension, d	2	3	4	5	7	8	9	11	13	16
Maximal error level in case of using two bases, %	25	33.3	37.5	40	42.9	43.8	44.4	45.5	46.2	46.9
Maximal error level in case of using $d+1$ **bases, %**	33.3	50	60	66.7	75	77.8	80	83.3	85.7	88.2

In this attack, the intruder creates the maximal error level by intercepting all of the qudits resent along the quantum path.

It is seen that, in case of the *IR* attack, the maximal error level created by interception is much higher while using $d+1$ bases than while using only two bases. At $d \to \infty$ the maximal error level in the first and the second case approximates 100% and 50%. This means that using all of the $d+1$ bases in the protocol with $d-$ dimensional qudits increases the protocol resistance to the *IR* attack.

It is known, however, that the *IR* attack for protocols with qubits provides the eavesdropper with the lowest amount of information at all D; in other words, this attack is the weakest attack.

The half-transparent noncoherent attack against prepare-and-measure protocols with qudit transfer is considered in [2] for legitimate users using $d+1$ bases. According to [2], the expression for the mutual information between subject A and the intruder is

$$I_{AE}^{(d+1)}(D) = \log_2 d + (1-D)\left[f(D)\log_2(D) + (1-f(D))\log_2 \frac{1-f(D)}{d-1} \right], \tag{4}$$

where

$$f(D) = \frac{d-2D+\sqrt{(d-2D)^2 - d^2(1-2D)^2}}{d^2(1-D)}. \tag{5}$$

A similar half-transparent attack in case of legitimate users using two bases is considered in work (5). The expression for $I_{AE}(D)$ is

$$I_{AE}^{(2)}(D) = \log_2 d + F_E(D)\log_2 F_E(D) + (1-F_E(D))\log_2[(1-F_E(D)]/(d+1), \tag{6}$$

where

$$F_E(D) = (1-D)/d + (d-1)D/d + 2\sqrt{(d-1)D(1-D)}/d. \tag{7}$$

The power of the *IR* attack and the noncoherent half-transparent attack for $d=4$ and $d=32.$ is compared in Fig. 3.

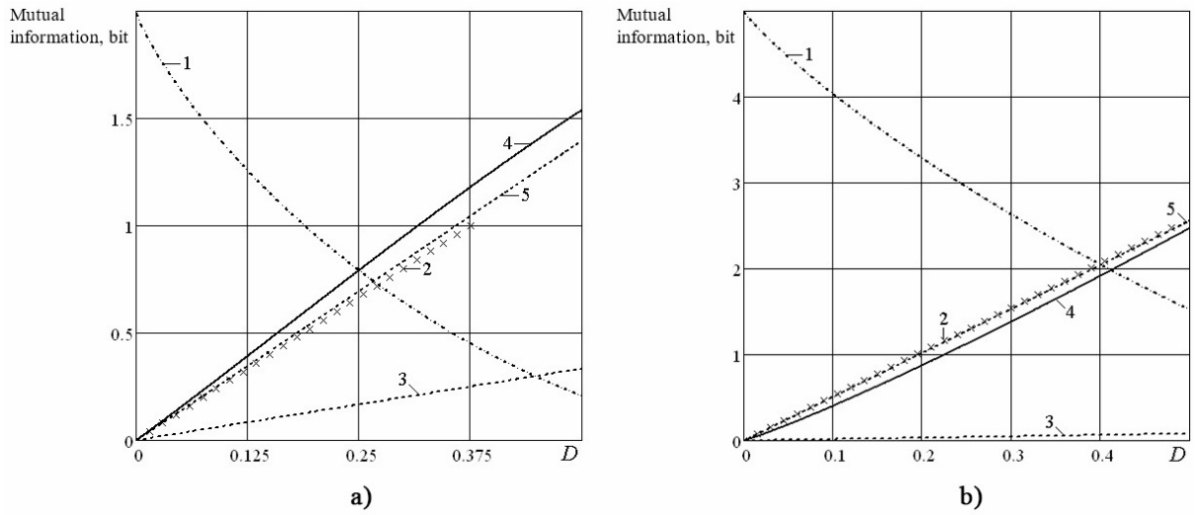


Fig. 3. Mutual information for the *IR* attack and for the noncoherent half-transparent attack:
a) $d=4$; *b*) $d=32$.
1 is $I_{AB}(D)$; 2 is $I_{AE-IR}^{(2)}(D)$; 3 is $I_{AE-IR}^{(d+1)}(D)$; 4 is $I_{AE}^{(2)}(D)$; 5 is $I_{AE}^{(d+1)}(D)$

It is seen that for the *IR* attack $I_{AE-IR}^{(d+1)}(D)$ is much lower than $I_{AE-IR}^{(2)}(D)$ like it should be: thus, for example, at $d=32$ in the first and the second case the intruder identifies one of 33 and, respectively, of only two bases. It should be emphasized that, when the protocol is implemented, subject *B* also identifies one of 33 and two bases, respectively; in other words, to generate the key, $1/33$ and a half of the transferred qudits can be used.

As for the half-transparent attack power, it is seen from Figure 3,*a* that, like at $d=2$ (see Figure 1 in [12]), at $d=4$ this attack is more powerful than the *IR* attack in the whole range of error level D in case of using $d+1$ and two bases. However, at $d=32$ (see Figure 3,b) the situation changes - in case of using $d+1$ and two bases, the half-transparent attack is somewhat weaker than the *IR* attack in case of using two bases. It should be noted that this transition takes place roughly at $d=16$ and this situation is fair for high d, too.

Now let us compare the power of half-transparent attacks for different d when the legitimate users use two or $d+1$ bases. Dependences $I_{AB}(D)$ (1), $I_{AE}^{(d+1)}(D)$ (4) и $I_{AE}^{(2)}(D)$ (6) for low d are shown in Fig. 4a. It is seen that at small qudit size and all values of D the curves for the protocols with $d+1$ bases (curves 4, 5, 6) are below the respective curves for the protocols with two bases (curves 7, 8, 9, respectively). This means that using all of the possible $d+1$ mutually nondisplaced bases in a protocol ensures a somewhat stronger resistance of this protocol to half-transparent attacks than using only two bases. However, like for the protocols with qubits [9,13,20], the difference in the information the intruder can have in case of using two or $d+1$ bases is small and the maximal value of this difference is only several percent (at a fixed D).

The same dependences for $d=16,\ 32$ and 64 are shown in Fig. 4b. It is seen that at $d=16$ (curves 4 and 7) the half-transparent attack provides the intruder with almost identical information up to $D\sim 0.5$, no matter whether the legitimate users use two or $d+1$ bases. The mutual information curves slightly diverge only at high D. At $d=32$ the intruder will have somewhat more information in a broad error level range D on condition that the legitimate users use $d+1$ bases (curves 5 and 8). At $d=64$ the intruder obtains more information in case of using $d+1$ bases already at all D (curves 6 and 9).

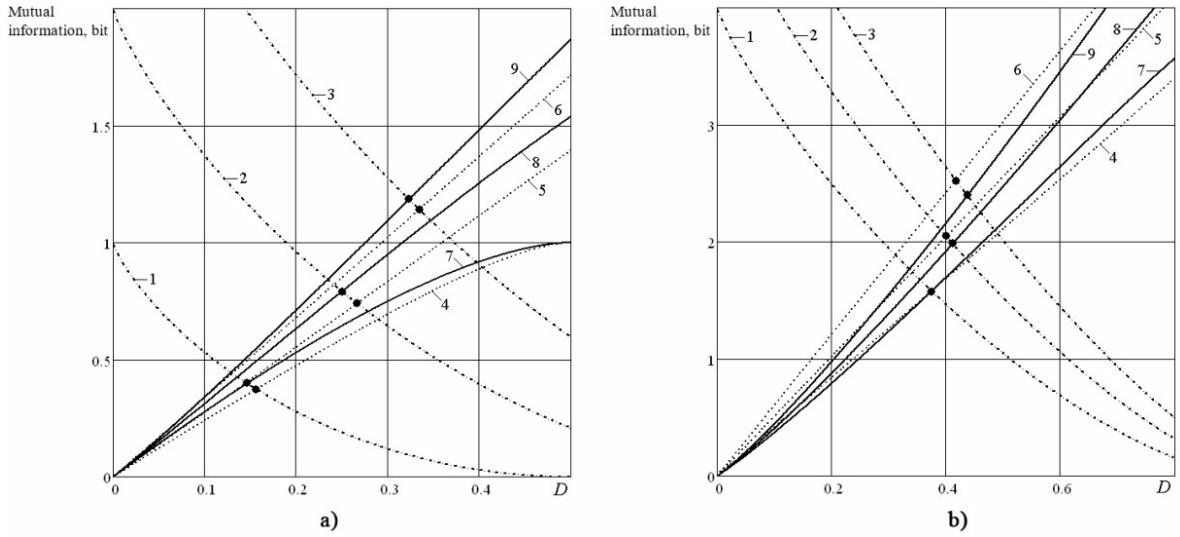


Fig. 4. Mutual information for the half-transparent noncoherent attack:

1, 2, 3 is $I_{AB}(D)$ (1) for $d=2$, 4, 8 (a) and $d=16$, 32, 64 (b);

4, 5, 6 is $I_{AE}^{(d+1)}(D)$ (4) for $d=2$, 4, 8 (a) and $d=16$, 32, 64 (b);

7, 8, 9 is $I_{AE}^{(2)}(D)$ (6) for $d=2$, 4, 8 (a) and $d=16$, 32, 64 (b)

Thus at small qudits of up to $d\sim 16$ the resistance of the prepare-and-measure protocol to half-transparent noncoherent attacks is stronger in case of using $d+1$ bases; at high d, however, the situation is opposite and the resistance of this protocol is stronger in case of using two bases.

In this case, if $d+1$ or two bases are used in the protocol, the difference in the information the intruder will know will be insignificant in its work region, that is, in the region of small error level D of legitimate users. It can therefore be concluded that, unlike in case of the *IR* attack, the number of bases used does not have much influence on the protocol resistance to the half-transparent attack, at least at a qudit size of $d=64$.

Thus the analysis shows that the resistance of prepare-and-measure protocols with multidimensional quantum systems to the *IR* attack and half-transparent noncoherent attack depends on the size of quantum systems (qudits) and on the number of mutually nondisplaced bases used by the users. At a small qudit size of $d\sim 16$ the half-transparent attack is stronger than the *IR* attack and the greatest difference in power between the attacks is registered for qubits. With an increase in d, the difference in power between the two attacks gradually decreases, when the legimate users use two bases, and virtually disappears at $d=16$. At a large qudit size and two bases used by the legitimate users the *IR* attack is more powerful than the half-transparent attack; with an increase in d the difference in power between the attacks slowly increases. Note that the weakest attack is the *IR* attack conducted with the use of $d+1$ bases by legitimate users; the power of this attack rapidly decreases with an increase in the size of the quantum systems in use. However, using $d+1$ bases also means an equally as fast reduction in the information capacity of the key exchange protocol.

VI. PHOTON NUMBER SPLITTING ATTACK AGAINST PROTOCOL BB84 AND SIX-STATE PROTOCOL

First of all, consider the photon number splitting attack against protocol BB84 (8). The probability of a pulse containing n photons is determined by the Poisson distribution as

$$p_n = e^{-\mu}\frac{\mu^n}{n!}, \tag{8}$$

where $\mu-$ is the average number of photons per pulse.

In case of a quantum path with losses the probability that subject *B* will register *n* photons in the pulse is determined as

$$p_{n,loss} = e^{-\eta\mu}\frac{(\eta\mu)^n}{n!}, \tag{9}$$

where $\eta-$ is the transfer coefficient of the path.

The probability of registering more than one photon in the pulse is determined as

$$p_{n>1,loss} = 1-e^{-\eta\mu}(1+\eta\cdot\mu). \tag{10}$$

Let us follow [8,18] and consider the following strategy of the pulse number splitting attack. The intruder blocks some part of k single-photon pulses and conducts a noncoherent attack against the other pulses. In its respect, the intruder withdraws a photon from each multiphoton pulse and thus calculates the exact bit value by measuring the sample state after the bases are declared.

Errors are generated in subject B only in case of the attack against nonlocked single-photon pulses the share of which is $1-k$.

The value of k is chosen so that the number of nonempty pulses expected by subject *B* for a path with losses is equal to the number of nonempty pulses after the intruder replaces the path with ideal path $(\eta=1)$ and blocks some part of single-photon pulses; in other words,

$$1-e^{-\eta\mu} = (1-k)p_1 + p_{n>1}, \tag{11}$$

where from the formula for calculating *k* is derived using formula (8) as

$$k = \frac{1}{\mu}\left(e^{\mu(1-\eta)}-1\right). \tag{12}$$

According to work [11], the probability that the intruder correctly measures the state of the sample mixed with a photon of subject *A* is calculated as

$$P_{correct} = \frac{1-e^{-\mu}(1+\mu)+(1-k)\mu e^{-\mu}\left(1/2+\sqrt{D(1-D)}\right)}{1-e^{-\mu}(1+\mu k)}. \tag{13}$$

Since the probability that the intruder incorrectly measures the sample state is $(1-P_{correct})$, $I_{AE}(D)$ for the described attack is

$$I_{AE}(D) = \frac{1}{2}\varphi\left[1-2(1-P_{correct})\right], \tag{14}$$

where function @ is determined as

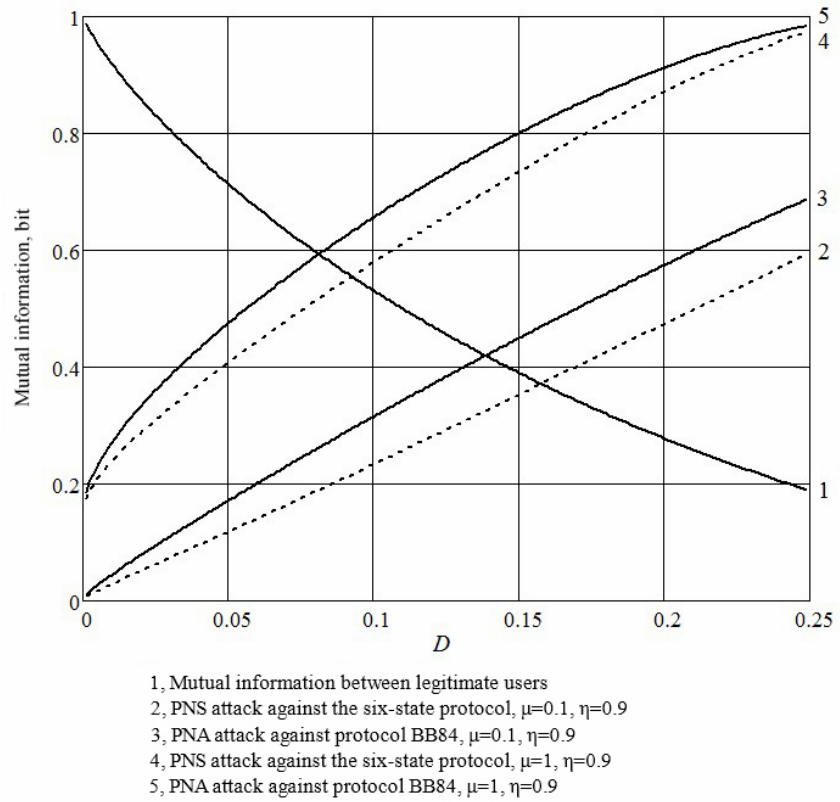
$$\varphi(z) = (1-z)\log_2(1-z)+(1+z)\log_2(1+z). \tag{15}$$

Note that mutual information equation (14) for the photon number splitting attack against protocol BB84 was earlier calculated in work [11]. However, the specialized literature provides no such expression for the six-state protocol.

We shall derive this expression considering that the intruder uses the above described strategy for the photon number splitting attack against the six-state protocol. For this purpose, expression $1/2+\sqrt{D(1-D)}$, that describes the noncoherent half-transparent attack against BB84 and corresponds to the attack of the intruder against single-photon pulses, should be replaced with the respective expression for the six-state protocol, that is, $1/2\left(1-D-\sqrt{D(2-3D)}\right)$ [2]. Then the mutual information between subjects *A* and *E* in case of the photon-number splitting attack against the six-state protocol is described with this same expression (14); but $P_{correct}$ is determined as

$$P_{correct}^{(6st)} = \frac{1-e^{-\mu}(1+\mu)+(1-k)\mu e^{-\mu}\left(1/2\left(1-D-\sqrt{D(2-3D)}\right)\right)}{1-e^{-\mu}(1+\mu k)}. \tag{16}$$

Curves $I_{AE}(D)$ in the photon number splitting attack against protocol BB84 and the six-state protocol at different average numbers of photons per pulse are shown in Fig. 5.



1, Mutual information between legitimate users
2, PNS attack against the six-state protocol, μ=0.1, η=0.9
3, PNA attack against protocol BB84, μ=0.1, η=0.9
4, PNS attack against the six-state protocol, μ=1, η=0.9
5, PNA attack against protocol BB84, μ=1, η=0.9

Fig. 5. Mutual information upon the photon number splitting attack against protocol BB84 and the six-state protocol

It is seen from Fig. 5 that the six-state protocol has a somewhat better resistance to the PNS attack than protocol BB84. Thus, at an average number of about 0.1 photons per pulse as well as in case of using a quantum path with low losses $(\mu = 0,9)$ the legitimate user can set a secret key on condition that the transfer error level does not exceed ~16% (crosspoint of curves $I_{AB}(D)$ and $I_{AE}(D)$, according to Csiszar-Korner theorem [6]). This is only by 2% higher than the similar indicator of protocol BB84 and the cost of this low additional resistance is the much smaller information capacity of the six-state protocol and, therefore, a lower key exchange speed.

Thus the protocol using three bases (six-state protocol) shows a stronger resistance to the photon number splitting attack than the protocol using two bases (BB84). However, the difference in resistance is small and does not exceed several percent. This result can be also spread to protocols with multilevel quantum systems, namely the protocol using $d+1$ bases will have a somewhat stronger resistance to the photon number splitting attack than the protocol using two bases. However, this small advantage in resistance does not compensate the far smaller information capacity of the protocol with $d+1$ bases in comparison against the protocol with two bases.

VII. RESULTS

The respective information capacities of prepare-and-measure protocols using two and $d+1$ bases are $\frac{\log_2 d}{2}$ and $\frac{\log_2 d}{d+1}$ bit/qudit, whereas the information capacity of protocols with mixed qudits (7) is $\frac{\log_2 d}{8}$ bit/qudit. The information capacities of prepare-and-measure protocols and protocols with mixed qudits for $d = 2\ldots16.$ are shown in Table 2.

Table 2. Protocol information capacity, bit/qudit

d	2	3	4	5	7	8	9	11	13	16
Prepare-and-measure-protocol, 2 bases	0.5	0.792	1.0	1.161	1.404	1.5	1.585	1.73	1.85	2.0
Prepare-and-measure-protocol, *d*+1 bases	0.333	0.396	0.4	0.387	0.351	0.333	0.317	0.288	0.264	0.235

Protocols with mixed qudits	0.125	0.198	0.25	0.29	0.351	0.375	0.396	0.432	0.463	0.5

It is seen that at $d < 7$ the information capacity of the prepare-and-measure protocols exceeds the information capacity of the protocols with mixed qudits, while at higher d the information capacity of the former protocols using $d+1$ bases is smaller than the information capacity of the latter but remains higher in case the former protocols use two bases. Therefore, at small d the information-measurement protocols have better efficiencies than the protocols with mixed qudits, whatever the number of used bases. At large d the prepare-and-measure protocols with two bases have the highest information capacity, protocols with mixed qudits have a smaller capacity, whereas the prepare-and-measure protocols with $d+1$ bases have the smallest information capacity.

According to the above analysis and the results of work, all of the three types of quantum key exchange protocols show a roughly equal resistance to the half-transparent noncoherent attack. In addition, it follows from the results of the preceding section of the work that the prepare-and-measure protocols with $d+1$ bases show an insignificantly better resistance to the photon number splitting attack than the protocols with two bases.

However, the protocols with two bases have a much greater information capacity than the two other types of protocols, whatever is dimension d of the Hilbert space of the quantum systems used to implement the protocol. Thus the conclusion of work can be generalized for the photon number splitting attack: the most optimal of all of the types of protocols with multidimrensional quantum systems in terms of information capacity and resistance to noncoherent attacks are prepare-and-measure protocols with two mutually nondisplaced bases.

VIII. CONCLUSION

In the article, on the basis of system analysis and modeling of the information parameters of the functioning of the qudit, a study of three types of quantum protocols for key distribution with the transmission of qudits, i.e. "preparation-measurement" type using $d+1$ and two mutually unbiased bases and protocols with interchanged qudits - simultaneously according to the criteria of the information capacity of the protocol and its resistance to incoherent attacks and the photon number separation attack in order to determine the optimal type of protocols. For the first time, the case of an attack with splitting the number of photons, as well as the stability of the protocol of its operation with six states, which belongs to the type of protocols with $d+1$ bases, is analyzed.

It is shown that the resistance to a semitransparent incoherent attack of protocols of the “preparation-measurement” type and protocols with entangled qudits is approximately the same, and the resistance of protocols of the “preparation-measurement” type with $d+1$ bases to the attack of splitting the number of photons is only slightly higher than the resistance to this attack of protocols with two bases. Taking into account the significantly higher information capacity of protocols of the “preparation-measurement” type with two bases compared to the other two types of protocols studied, it was concluded that, simultaneously, according to the criteria of information capacity and resistance to incoherent attacks and the attack of splitting the number of photons, protocols of the “preparation-measurement” type with two bases are optimal.

It should be noted that quantum cryptography is one of the areas of information protection, offering new methods for ensuring the confidentiality of information, the strength of which is based on the laws of quantum physics and, under certain conditions, is information-theoretic. The development of new protocols for quantum secure communication with increased information capacity, analysis of their resistance to attacks, as well as determination of the best protocols according to the criteria of stability and information capacity in the group of similar quantum cryptography protocols are topical scientific problems of great theoretical and practical importance and require further research.

This work was supported by the Azerbaijan Science Foundation – grant no. AEF-BQM-BRFTF-4/2024-5(53)-06/02/1-M-02.

REFERENCES

[1]. Bourennane, M. Quantum key distribution using multilevel encoding / M. Bourennane, A. Karlsson, G. Bjork // Quantum Communication, Computing, and Measurement 3. – N.Y.: Springer US, 2002. – P. 295 – 298. https://doi.org/10.1103/PhysRevA.64.012306

[2]. Bruss, D. Optimal Eavesdropping in Quantum Cryptography with Six States / D. Bruss // Physical Review Letters. – 1998. – V. 81, issue 14. – P. 3018–3021. https://doi.org/10.1103/PhysRevLett.81.3018

[3]. Bruss, D. Optimal eavesdropping in cryptography with three-dimensional quantum states / D. Bruss, C. Macchiavello // Physical Review Letters. – 2002. – V. 88, issue 12. – 127901. https://doi.org/10.1103/PhysRevLett.88.127901

[4]. Benenti, G. Principles of Quantum Computation and Information. Vol. 1: Basic Concepts / G. Benenti, G. Casati, G. Strini. – World Scientific, 2004. – 267 p.

[5]. Cerf, N.J. Security of quantum key distribution using d-level systems / N.J. Cerf, M. Bourennane, A. Karlsson, N. Gisin // Physical Review Letters. – 2002. – V. 88, issue 12. – 127902. https://doi.org/10.1103/PhyRevLett.88.127902

[6]. Csiszar, I. Broadcast channels with confidential messages / I. Csiszar, J. Korner // IEEE Trans. on Inform. Theory. –1978. – V. IT-24, № 3. – P. 339–348. https://doi.org/10.1109/TIT.1978.1055892
[7]. Durt, T. Security of quantum key distributions with entangled qudits / T. Durt, D. Kaszlikowski, J.-L. Chen, L.C. Kwek // Physical Review A. – 2004. – V. 69, issue 3. – 032313. https://doi.org/10.1103/PhysRevA.69.032313
[8]. Gisin, N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Review of Modern Physics. – 2002. – V. 74, issue 1. – P. 145–195. https://doi.org/10.1103/RevModPhys.74.145
[9]. Hwang, W. Eavesdropper's optimal information in variations of Bennett-Brassard 1984 quantum key distribution in the coherent attacks / W. Hwang, D. Ahn, S. Hwang // Physics Letters A. – 2001. – V. 279, issues 3–4. – P. 133–138.
[10]. Lutkenhaus, N. Estimates for practical quantum cryptography / N. Lutkenhaus // Physical Review A. – 1999. – V. 59, issue 5. – P. 3301–3319. https://doi.org/10.1103/PhysRevA.59.3301
[11]. Niederberger, A. Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography / A. Niederberger, V. Scarani, N. Gisin // Physical Review A. – 2005. – V. 71, issue 4. – 042316. https://doi.org/10.1103/PhysRevA.71.042316
[12]. Vasiliu, E.V. Analytical Comparison of Key Exchange Protocols with Transfer of Multidimensional Quantum Systems for Efficiency and Resistance to Noncoherent Attacks / E.V. Vasiliu, R.S. Mamedov // Scientific Papers of O.S. Popov Odessa National Academy of Telecommunications. 2008. Issue 2. Pp. 20–27.
[13]. Vasiliu, E.V. Resistance of Prepare-and-Measure Quantum Key Exchange Protocols. Georgian Electronic Scientific Journal: Computer Science and Telecommunications / E.V. Vasiliu // 2007. Issue 2(13). Pp. 50-62.
[14]. Zenevich, A.O. Fiber optic coupler. Patent for invention No. 23638 / A.O. Zenevich, A.A. Lagutik, T.M. Lukashik, T.M. Mansurov, E.T. Mansurov, E.V. Novikov // National Center for Intellectual Property of the Republic of Belarus. – Minsk, 2022 from 24.03. 2022. - 7p.
[15]. Mansurov T.M. Fiber optic coupler. Patent for invention No. İ 2022 0032 // T.M. Mansurov, A.O. Zenevich, I.A. Mamedov, E.V. Novikov, E.T. Mansurov // Intellectual Property Agency of the Republic of Azerbaijan. -Baku, 2022 from 13.05.2022. -11p.
[16]. Bennett, C.H. Quantum cryptography using any two nonorthogonal states / C.H. Bennett // Physical Review Letters. – 1992. – Vol 68, Iss. 21. – P. 3121–3124.
[17]. Scarani, V. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf [et al.] // Review of Modern Physics. – 2009. – Vol. 81, Iss. 3. – P. 1301–1350.
[18]. Lutkenhaus N. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack / N. Lutkenhaus, M. Jahma // New Journal of Physics. – 2002. – Vol. 4. – P. 44.1–44.9.
[19]. Bruss, D. Quantum Key Distribution: from Principles to Practicalities / D. Bruss, N. Lutkenhaus // Applicable Algebra in Engineering, Communication and Computing. – 2000. – Vol. 10, № 4–5. – Pp. 383–399.
[20]. Scarani, V. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf [et al.] // Review of Modern Physics. – 2009. – Vol. 81, Iss. 3. – Pp. 1301–1350.
[21]. Lo, H.-K. Quantum cryptography / H.-K. Lo, Yi Zhao // Encyclopedia of Complexity and Systems Science. – N.Y.: Springer US, 2009. – Vol 8. – Pp. 7265–7289.
[22]. Dusek, M. Quantum Cryptography / M. Dusek, N. Lutkenhaus, M. Hendrych // Progress in Optics. – Vol. 49. – «Elsevier», 2006. – Pp. 381–454.
[23]. Caruso, F. Robustness of a quantum key distribution with two and three mutually unbiased bases / F. Caruso, H. Bechmann-Pasquinucci, C. Macchiavello // Physical Review A. – 2005. – Vol. 72, Iss. 3. – 032340.
[24]. Jung, E. Attack of many eavesdroppers via optimal strategy in quantum cryptography / E. Jung, M.-R. Hwang, D.-K. Park [et al.] // Physical Review A. – 2009. – Vol. 79, Iss. 3. – 032339.