INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2006 情財第 0201 号

イスラエルにおけるセキュリティ関連動向調査報告書

The research and development trends in the Quantum Key Distribution (QKD) Systems in Israel

2007 年 3 月
独立行政法人 情報処理推進機構

Overview:

This report will relate to the following subjects:

The research and development trends in the Quantum Key Distribution (QKD) Systems in Israel:

1. Quantum Key distribution
    a. R&D organizations
    b. Performance
    c. Sale situation
    d. Export control

2. The research and development trends of the main devices used in Quantum Key Distribution (QKD) Systems in Israel for Single photon source, Photon detector, Polarization Elements:
    a. R&D organizations
    b. Performance
    c. Sale situation
    d. Export control

- The list of R&D organizations and the names of the researchers indicated in the report relate to both subjects together; the QKD trend and Single Photon Source.
- The Export Control situation is detailed in the report for both subjects; the QKD trend and Single Photon Source.

Table of contents:

1. Opening for QKD

The security of Key Distribution inherent risks in the current encryption technologies such as DES, RSA and other systems. All existing classical crypto-systems are not proven to be secure. Their security is based on computational complexity assumptions which sometimes turn out to be false.

Daily, we hear about hackers who manage to break into the most secure computer systems of known institutes, government offices, different agencies, secured networks, companies and private computers. This issue brings many researchers in the academic and industrial world to develop new security systems using huge investments to overcome these problems and constantly look to develop new and advanced encryption standards.

It seems that all these efforts are not enough, and still there are problems that the classical security does not solve. The researchers believe that complex of protocols encryptions with a quantum computer will be the answer to the security problem and bring more security in the field of communication. The fact that a quantum-based computer can perform instructions so much faster than current computers, will serve both sides the sender-receiver and the attacker. The intruders can use such technology to reduce cracking time and render algorithms which are used today in the classical system. Obviously, when quantum-based computers become reality, stronger algorithms will be needed to protect information. The answer is the quantum encryption.

The objective of quantum cryptography is to provide protocols that are secure against an adversary equipped with any computational power.

There are many protocols mentioned in the enclosed report which were written by Israeli researchers. Some simple and some complicated, all of them have a common target to develop security to defend communication between two or more parties from different attacks and to be able to use them against any eavesdropping attempt.

The efforts that are made for developing security of QKD against sophisticated attacks in the classical systems is among the most important issues in quantum information theory. In Israel, all the main universities and some institutes are researching the security of quantum key distribution.

These researches are sometimes done by a group of researchers which consist of Israeli researchers and sometimes foreign researchers that join together to make the research.

2. R&D Organizations

Universities, Institutes and the main researchers in each organization:

1) Technion, Israel Institute of Technology, Haifa
   i. Dr. Tal Mor- Computer Science Department
   ii. Prof Biham- Computer Science Department
   iii. Dr. Daniel Terno- Physics Department
   iv. Prof. Amit Ben Kish- Physics Department
   v. Prof Oded Regev- Astrophysics
2) Hebrew University, Jerusalem
   i. Prof Michael Ben-Or, Computer Science and Engineering department
   ii. Dr.Dorit Aharonov- Department of Computer Science & Engineering
   iii. Prof. Uri Banin- Nano-Science research group
   iv. Dr. Hagai Eizenberg- Department of Computer Science & Engineering
3) Tel Aviv, University
   i. Prof Lev Vaidman, School of Physics and astronomy
4) Bar Ilan University, Tel Aviv
   i. Prof. Eli Barkai- Physics department
5) Ben Gurion University, Beer Sheva
   i. Dr. Ron Folman- The Atom Chip Lab
   ii. Dr. Gershoni- Solid State Institute
   iii. Dr. Motti Gabay – Satellite and wireless communication laboratory
   iv. Dr. Shlomi Arnon– Satellite and wireless communication laboratory

6) The Weizman Institute

i. Prof. Oded Goldreich, Computer Science at the Faculty of Mathematics and Computer Science

Prof Ben-Or from the Hebrew University and Dr. Tal Mor from the Technion Israel Institute of Technology with their associates took the time and efforts to proved the security of QKD.

All the researchers in the above mentioned institutes are continuing to research and develop new security possibilities in the QKD field.

3. Performance:

In this part, we will analyze the performance that has been done for the proofs for security of Quantum Key Distribution (QKD) in Israel and analyze some of the more important researches in this subject.

All the information brought forward was taken from the researches that are enclosed to this report and are mentioned in the references.

1) The Advantages of the Quantum Key Distribution (QKD)

The main advantage of the quantum cryptography system is that in the quantum system the security has been proved. On the other hand, the security in classical system which is based on complexity of mathematical systems can be dissolved and by quantum computers it will be even easier to dissolve. The power of quantum cryptography will overcome any sophistication of any eavesdropper. In the future more and more quantum cryptographic systems will be used in communication systems.

One of the most important quantum cryptographic applications is QKD. Classically, KD cannot be unconditionally secured (i.e. secure against all possible classical attacks). Furthermore, the security of existing KD schemes is based on assumptions that computation complexity has limitations of the memory space of the adversary. In contrast, QKD is based on intrinsic quantum mechanics, which allows eavesdropping activities to be detected in principle. Indeed, QKD can be unconditionally secure against eavesdropping capability since the QKD system can trace the interference of an eavesdropper by measuring the noise in the channel. In general, QKD remains secure even if the quantum states are sent through a noisy quantum

channel, as long as the observed error rates are below certain threshold values.

2) The Target of Key Distribution (KD)

The target of KD is to enable two remote parties to share a secret bit string such that no third party, Eve, will have much information about the bit string. Classically, KD can not be unconditionally secured unless Alice and Bob can identify one another and detect alteration in their communication. In the classical way Alice and Bob have to identify one another and detect alterations in their communication. In other words, the task of message authentication is necessary for KD. There are unconditionally secure methods for authenticating a classical message with a shorter key. Thus, KD uses authentication as a subroutine, and achieves key expansion. Classical physics permits an eavesdropper to have exact duplicates of all communications in any KD procedure without being detected. In contrast, while QKD cannot prevent eavesdropping, it can detect it. As a result, Alice and Bob can abort the key or the total communication. The usefulness of QKD is to avoid Alice and Bob being fooled into having a false sense of security. QKD does not promise to always produce a key, since Eve can be detected and the communicating parties will need to abort their communication.

3) Quantum Key Distribution – Basic Knowledge

Quantum encryption systems use lasers to generate individual pulses of light called photons. Each photon is sent in one out of four modes, as specified in the protocol BB84, either vertical/horizontal, or plus 45 degrees/minus 45 degrees. Within each mode, one orientation represents the digital value 0, and the other represents the digital value 1. To better understand how it works, one can imagine that each photon is a tiny envelope moving perpendicular to the ground (vertical=1), parallel to the ground (horizontal=0), tilted at 45 degrees to the right (plus 45 degrees =1) or tilted 45 degrees to the left (minus 45 degrees=0). In other words, Alice sends to Bob a chain of photons. Each one of them is polarized in one of the four positions of BB84.

Alice randomly chooses both a mode and a digital value or orientation for each photon sent over the quantum channel. Bob randomly chooses between the two modes when he tries to detect a photon. This can be visualized as choosing a mailbox slot that accepts only envelopes flying in certain orientations. If he chooses the same mode that Alice used for a particular photon, then Bob always measures the correct orientation, and hence, its digital value. But if he chooses a different mode, then he may get the wrong value for that photon.

To remove this uncertainty, Alice uses another channel which is a standard wireless Ethernet channel to tell Bob which mode she used for each photon, but not its digital value. Bob ignores those instances for which he measured a photon in the wrong mode, and tells Alice which ones he measured correctly (but again, not their bit value) so she can also discard the

ones Bob did not measure correctly. The correct measurements constitute the encryption key that Alice and Bob now share.

For example, if Alice chooses to send a photon in the vertical/horizontal mode and with the digital value 1, then she orients it vertically and sends it to Bob. If, when the photon arrives at Bob, he chooses the vertical/horizontal mode to measure it, then his measurement will necessarily only show that it is a vertically oriented photon, and he will record a 1. If he uses the plus 45 degree/minus 45 degree mode, then his measurement has an equal chance of yielding a 0 or a 1, but nevertheless he will record the result. After a short time, Alice tells Bob that this photon should have been measured in the vertical/horizontal mode. If he used this mode then he knows his measurement was correct, and he adds the digital value to his key, and he tells Alice that he measured this photon correctly so she can keep that value as well. But if he used the other mode, or if the photon never arrived, then he tells Alice to discard the value of that photon.

In real operation, the vast majority of the photons never arrive at Bob. But, as can be seen from the example above, even those that do reach Bob have only a 50/50 chance of being measured in the correct mode. It is only the photons that arrive at Bob, and are measured in the correct mode, that contribute to the key shared by Alice and Bob. Ignoring sources of noise in the channel, at this point Alice's and Bob's keys are identical. Because the standard wireless Ethernet channel system is capable of sending quantum bits so fast that a large number of photons can be lost or thrown away because Alice and Bob's modes do not match and yet there are still plenty of digital values to produce a secure encryption key.

If someone, as Eve, tries to eavesdrop on the transmission, she will not be able to "read" it without altering it. Eve must randomly position her receiver to intercept Alice's transmission. The photon is converted to electrical energy as it is measured and destroyed, so Eve must generate a new quantum message to send to Bob, but she must guess a significant number of the digital values. These guesses cause errors in the string of digital values used as the encryption key shared by Alice and Bob. By comparing small quantities of their digital key values, Alice and Bob can look for these errors. If they find more differences than can be attributed to known sources, they will know that there is an eavesdropper on the channel and they will discard the key.

4) Characteristics of Quantum Key Distribution

The main characteristics of QKD is that, a key distributed via quantum cryptography techniques is secure even against an eavesdropper with unlimited computing power, while the most advanced “public key” or “secret key” schemes do not have, and never will have, this type of security. Using quantum two-level systems, qubits, instead of classical bits has lead to many surprising results such as exponentially fast quantum algorithms, teleportation of unknown states and quantum cryptography. QKD protocol which was presented in 1984 by Bennett and Brassard came to provide a new type of solution to one of the most important cryptographic problem: the transmission of secret messages between at least two remote parties.

5) Broadcasting Messages

Alice and Bob use qubits for their quantum communication, and they have access to a classical communication channel which can be heard, but

cannot be jammed by an eavesdropper. Alice and Bob can broadcast messages, if they already share some small number of secret bits in advance they can authenticate each other by classical channels, after receiving the bit string which was sent by Alice to Bob.

6) Error Rate

Alice and Bob must use an un-jammable classical channel to inform each other which bits were identified conclusively and to compare some of the common bits in order to estimate the error rate. They must accept some small error rate due to imperfection in creating, transmitting and receiving the quantum states. The estimate error rate should not exceed the agreed error rate as if it will exceed, the parties will need to quit the transmission and will not use the data. Thus any eavesdropping attempt is severely considered to induce an error rate smaller than what is allowed. Each of the researchers who proved the security of QKD, prove in their protocol different levels of error rate.

7) The Distance of Communication Using QKD

At this time, when QKD is still in the R&D stage, one of the main problems is how far the key of the quantum cryptography can go. In 2006, the researchers succeeded to make connection between Alice and Bob at approximately 100km. For comparison, at the beginning of 2003, the distance was only 25km which means each year the researches succeed to double the distance that they succeed to send the key for quantum cryptography. The researches found that quantum-encoded transmission can be established to and from low-orbiting satellites, enabling completely secure communications between any two points on earth.

Quantum encryption keys are based on the laws of quantum mechanics and unlike other encryption codes which are based on mathematical number theory, they are impossible to intercept or break. As a result, two parties can use a successfully transmitted key to encode and decode secure messages with complete confidence.

8) The Quantum Encryption Conception

The quantum technology will effect and change the whole concept of encryption. Following are the reasons:

i. QKD uses the power of quantum mechanics to suggest the distribution of a key that is secure against an adversary with unlimited computation power. Such a task is beyond the ability of classical information processing.

ii. The extra power gained by the use of quantum bits (quantum two-level systems "qubits") is due to the fact that the state of such a system cannot be cloned. On the other hand, the security of conventional key distribution is based on the (unproven) existence of various one-way functions, and mainly on the difficulty of factoring large numbers, a problem which is assumed to be difficult for a classical computer, and is proven to be easy for a hypothetical quantum computer.

iii. From the attacker's point of view, there are several classes of attacks on QKD that can be performed by having full control of the channel. The simplest ones are known as individual-particle attacks in which the transmitted qubits are attacked separately, so that the attacker can be left with some optimal classical information about each transmitted

quantum bit. The attacker can use this classical information in order to learn some information about the final secret key. In contrast, in the most general attack, called the "joint attack", all transmitted quantum particles are attacked together, the attacker's goal is to learn as much information as possible about the final key, rather than about each transmitted qubit. A special class of the joint attack, the "collective attack", was shown to provide more information to the attacker than an individual-particle attack. According to the proof, the honest side can abort his activities whenever he senses an attack, by this the attacker can not get any information.

iv. Another reason that encryption concept will totally change is due to the proofs that relate to security of all the existing Public Key Distribution that can be broken. The research done today continues to prove the ultimate security of QKD against any attack. Note that the eavesdropper is assumed to have unlimited technology (e.g. unlimited computing power, a quantum memory, quantum computer), while the legitimate users use practical tools (or, more precisely, simplifications of practical tools). Such assumptions are required since the aim of the invention of QKD is to obtain a practical key distribution scheme, which is proven secure against any attack, even one which is far from being practical with current technology.

9) Randomness Provides Security

The Technion's researchers obtained new information for disturbance results, where the power of quantum information theory is manifested in an intuitive and clear way. They show explicitly how the randomness of the

choice of bases and the randomness of the choice of test-bits provides the desired security of QKD.

The Technion's group adopted and generalized sophisticated tools invented in "Purification" which simplify Eve's states, bound on accessible information (using Trace-Norm-Difference of density matrices) which avoids any complicated optimization of Eve's possible measurements, and a connection between Eve's accessible information and the error-rate she induces.

The Technion's proof analyzes the density matrices which are available to the eavesdropper and prove that it is extremely rare that these density matrices carry non-negligible information about the secret key. It is extremely rare that Alice and Bob agree to form a secret key about which these density matrices reveal non-negligible information.

10) Basic Assumptions for the Proof of Security in QKD:

i. The Technion's group assumed the correctness of quantum theory.
ii. Alice and Bob share an un-jammable classical channel. This assumption is usually replaced by the demand that the classical channel is "un-forgeable"; an un-forgeable channel can be modified by an eavesdropper but Alice and Bob will notice that, with probability exponentially close to one.
iii. Another assumption is that Eve cannot attack Alice and Bob's laboratories. She can only attack the quantum channel and assumes that she can listen to all transmissions on the classical channel.

iv. Alice sends quantum bits, i.e. two level systems. This assumption cannot be fully met in any experimental scenario, but can only be approximated.

v. The Technion's researchers prove, under those assumptions, the security of the BB84 protocol, against any attack allowed by the rules of quantum physics. They prove security for instances in which the error rate in the transmission from Alice to Bob is up to 7.56%.

11) The Four States of the BB84 Protocol

Four states are defined in Protocol BB84, such that the first two are orthogonal in one basis, and the other two are orthogonal in another basis. The two bases are conjugate, namely, applying a measurement in one basis on a state belonging to the other basis gives a fully random outcome. In the BB84 protocol Alice and Bob use these four possible quantum states.

The BB84 protocol contains one step in the part of quantum communication, Alice sends Bob a randomly string of qbits each in one state. The researchers assume all qubits are sent to Eve, and then Eve sends all qubits to Bob. The reason is that incase Eve can only hold each qubit for a short time and must release it before she gets the next, she is less powerful, so the proof of security covers that case as well.

The rest of the process involves sending classical communication via the un-jammable channel. First Alice sends Bob the basis used for each photon. By comparing bases after Alice sends such a state for each qubit and Bob receives the qubit, a common key can be created in instances when Alice and Bob used the same basis. Comparing the bases must be performed

after Bob receives the qubits, so that the eavesdropper cannot benefit from having this knowledge while still holding the qubits. The common key obtained from the steps is known as the “sifted key”. A final key is then obtained from the sifted key, after performing several more steps: testing the error rate on some test bits, chosen at random; throwing away these test bits, while Alice and Bob can now have some good estimation of the error-rate on the remaining shared bits, correcting errors on these information bits, and amplifying the privacy, by creating a shorter final key. Alternatively, if Bob has a memory where he can keep his qubits unchanged after receiving them (such a memory is called “a quantum memory”), a simpler protocol for obtaining a sifted key is obtained: Bob waits with the received qubits till he learns the basis, and then measures in the right bases. The sifted key is twice as big in this case or the initial string of qubits can be shortened to half, if the final length of the sifted key is to remain the same.

The Technion’s researchers prove here the security of that simplified protocol in which only the bits relevant for the sifted key are discussed; it is called the “used-bits-BB84”. The proof of the security of the original BB84 protocol (in which Bob does not have a quantum memory) easily follows due to a simple reduction.

12) The Sifted Key

Sifted key is generated one step before the final key, this means that after Alice sends Bob randomly 2*n* Bit Stings and Bob receives them and tells Alice about it. Alice publishes the basis she used, Bob measures the qubits according to Alice's basis to obtain identical a 2*n* bit sting. The result

of these measurements is a sifted key which means Alice and Bob have identical bit strings.

The group of researchers from Technion showed that the key generated by the sifted key is reliable: the keys distilled by Alice and Bob (after error correction and privacy amplification) are identical except for some exponentially small probability.

13) The Process of Creating the Final Key

i. A $2n$-bit string which was chosen in the stage of creating the sifted key is the basis of creating the final key which has exactly n zeros and n ones.
ii. Alice selects a subset of n bits, to be the test bits and publishes the string, along with the values of the test bits. Later, Alice will send error-correction codes and privacy-amplification information to Bob, than Bob needs to correct his errors using the error-correction codes data, and to obtain a final secret key equal to Alice's using the privacy-amplification data.
iii. Bob checks with Alice that the error-rate in the test bits is lower than some pre-agreed allowed error-rate, and aborts the protocol if the error-rate is larger.
iv. Bob also publishes the values of his test bits. This is not crucial for the protocol, but it is done to simplify the proof.
v. Alice also announces the bit string which is her information string and accordingly Bob performs the correction on his information bit string.

The researchers offer a strategy to check the final key:

vi. The strategy is as follows:

a. Alice announces parity-check matrix. Alice announces the bit string whose bits are the parity's of her information strings.
b. Bob performs the correction on his information bits. Bob finds the right strings.
c. Alice selects privacy amplification and publishes it.
d. Bob finally calculates and gets the key.

14) Eve's Observation

Eve can attack the qubits in two different stages. First she lets all qubits pass through a device that weakly probe their state via a quantum unitary transformation. Then, after receiving all the classical data, she measures the probe. Note that Eve can gain nothing by measuring the probe earlier, or by measuring the qubits while passing through her. Any such measurement can also be performed by attaching a probe, applying a unitary transformation, and measuring the probe (or part of it) at a later stage. Since there is no gain in performing a measurement before learning all the classical information that is transmitted throughout the protocol, the optimal attack (without loss of generality) is to perform all measurements after receiving all classical information.

Furthermore, Eve gains nothing by sending Bob a state that is not a $2n$ qubit state, so without loss of generality, we assume she sends exactly $2n$ photons: If Eve sends less than $2n$ qubits, Bob will add the missing qubits in an arbitrary state so Eve could have done it herself. If Eve sends more than $2n$ qubits, Bob ignores the extra qubits, and again Eve could have done it herself. (An important remark though: the allowed error-rate in these cases

must still be limited. However, in real applications the natural losses of qubits become very high due to transmission across long distances. If one does not wish to limit the distance too much, and wishes to have security even if losses are much higher than allowed, then this is still possible.

It is important to enable an analysis of Eve's most general attack. Thus we formally split Eve's attack into her transformation and her measurement. Eve's transformation, Eve attacks the qubits while they are in the channel between Alice and Bob. Eve can perform any attack allowed by the laws of physics, the most general one being any unitary transformation on Alice's qubits and Eve's probe.

The situation is generous to Eve, allowing her to attack all the qubits together (in practice, she usually needs to release the preceding qubit towards Bob before she has access to the next one). Without loss of generality it is assumed that all the noise on the qubits is caused by Eve's transformation.

In individual-particle attacks and in collective attacks Eve's transformation is restricted so that each transmitted qubit is attacked using a separate, un-entangled probe, so that the analysis is simplified. In collective attacks the next step is as general as it is for the joint attacks (so that Eve can measure all probes together). In contrast, in individual-particle attacks Eve is only allowed to measure each probe separately from the others.

15) Eve's Activities to Obtain the Final Key

First Eve can keep all the information she got from Alice and Bob in an unchanged state including the bases of all bits, she tries to guess the final key using her best strategy of measurement. Secondly, she can use the measurement by adding a second ancilla, and performing a standard projection measurement on her probe and the ancilla.

According to the researchers, in order to prove security this task does not need to be solved, and it is enough to find bounds on Eve's optimal information (via any operation she could have done). In order to analyze her optimal transformation the researchers find bounds for any transformation she could perform.

16) QKD Gives Freedom to the Legal Users

In QKD, Alice and Bob are supposed to start their communication with a small initial key for authentication purposes. They can use uncorrelated randomness that is not controlled by Eve. They may exchange quantum and classical messages in both directions via channels that are completely under the control of Eve, and may perform local quantum operations and measurements. Based on their measurement outcomes, Alice and Bob can decide if the QKD test is failed or passed and either abort QKD or generate their respective keys KA, KB correspondingly. Eve also obtains quantum and classical data from which she extracts classical data KE via a measurement. What happens during a specific run of QKD depends on the particular outcomes of quantum measurements of all the parties.

17) The Security of QKD Based on Protocols

Prof Ben-Or from the Hebrew University and his associates indicate various QKD protocols that are used to proof security: BB84, E91, B92, and the six-state protocol. These protocols demonstrate unconditional security of different error rates, by allowing only one-way classical communications in the error correction/privacy amplification procedure between Alice and Bob, which shows the advantage of the six-state scheme over the BB84.

18) The Different Possibilities for Attacking

There are different kinds of attack to get the secret which is shared between Alice and Bob. All the attacks depend on Eve, the attacker.

Proofs of security of QKD, address all attacks on the QKD scheme allowed by quantum mechanics. The problem is that QKD is not the only occasion for attack — further attack may occur when Alice and Bob use the keys generated. In particular, Eve may have never made a measurement during QKD to obtain any KE. Eve's transcript is a quantum state. She could have delayed measurements until after more attack during the application, a strategy with power that has no classical counterpart.

As it turns out, there are many other occasions in which joint attacks on QKD (attacking all the qbits together) and the subsequent use of the generated key by Alice and Bob have to be considered. For example, suppose Alice and Bob perform process QKD to obtain a key, and then use the key to encrypt quantum states. Eve eavesdrops during both QKD and encryption and performs a collective measurement on the two eavesdropped states. It is well-known that such a collective measurement may yield more

accessible information than the sum of information obtained in two separate measurements. Current study by the researchers is further motivated by the results in which show that there are ensembles of quantum states that provide little accessible information on their own, but can provide much more information when a little more classical data is available. The extra information can be arbitrarily large compared to both the initial information and the amount of extra classical data. Such strange property reveals a new, unexpected, inadequacy of mutual-information based statements. In particular, in the context of QKD, the usefulness of bounding the initial accessible information of Eve becomes very questionable, if Eve delays her measurement until further data is available during the application of the key, the security of the key is questionable even in classical applications.

19) Re-use of the QKD

One of the earliest known security problems in QKD is the requirement of a key for authentication, which may in turns come from a previous round of QKD. Since each run of QKD is slightly imperfect, repeated QKD produce less and less secure keys.

20) The Framework of Composability for Providing Security

Composability is concerned with the security of composing cryptographic primitives in a possibly complex manner. The simplest example is the security of using a cryptographic primitive as a subroutine in another application. For a specific task (functionality), a primitive that realizes the task is said to be universal composable if any application using the primitive is about as secure as using the ideal functionality. Universal

composability provides the precise framework for proving the security of using the keys generated from QKD.

Prof Ben-Or and his associates found potential security problems in using the keys generated from QKD. They define a new security definition for QKD that is universal composable (Appendix E). The principal is that QKD and certain ideal KD should be indistinguishable from the point of view of the potential adversaries. The researchers prove that the original mutual-information-based security definition implies the new composable definition. The researchers bring in their work other simple sufficient conditions for the composable security of QKD. One of these conditions high singlet-fidelity is an intermediate step in the widely-used "entanglement-based" security proofs of QKD. The researchers show that high singlet-fidelity is much more closely related to composable security than the usual security definition. They obtain better security connections for known QKD scheme. They also prove the security of using a key generated by QKD in various ways and provide simple criteria for future scheme.

The researchers work also has non-cryptographic applications in the study of correlations in quantum systems. The various security conditions are tied to correlation measures in quantum systems. Each derivation for the composable security for QKD is based on relating a pair of correlation measures.

21) Reversible Extracted Information

In quantum mechanics, one can only reversibly extract information from an unknown quantum state if the state is drawn from an orthogonal set.

For example, if Alice encodes her message using a random basis chosen from several non-orthogonal possibilities, and Eve is to obtain any information on the outcomes of KA, KB, then ρB ≠ Pa (p-the state). To detect the disparity, Bob measures some of the received qubits (the "test-qubits" chosen randomly to avoid Eve tailoring her attack) and discusses with Alice to check if his measurement outcomes are consistent with what Alice has sent. This intuition can be turned into a provably secure procedure. Alice and Bob estimate various error rates on the test-qubits. If the observed error rates are below certain threshold values, it is unlikely that the untested qubits have much higher error rates. Error reconciliation and privacy amplification are applied to extract bit-strings kA and kB for Alice and Bob respectively. If the observed error rates are above the thresholds, Alice and Bob abort QKD. QKD remains secure whether the observed noise is due to natural channel noise or due to eavesdropping.

22) Schemes for Generating QKD

The Prepare-&-measure schemes are the main scheme in generating the QKD but there are other schemes such as the entanglement-based QKD schemes. The basic components are still secure local coins, completely insecure quantum communication, and authenticated public classical communication between Alice and Bob. In the most general QKD scheme, the components may be used in any possible way. Alice and Bob still obtain some bit-strings as the output keys, kA and kB, of certain length m. Eve's view is still given by some quantum and classical data, denoted collectively by ρE, kA, kB, with explicit dependence on kA, kB.

It must be emphasized that there is a limitation in QKD. It is possible for Eve to be "lucky," for example, to have attacked only the untested qubits, or to have attacked every qubit without causing inconsistency in Alice and Bob's measurements. It is unlikely, but still possible, for Eve to have a lot of information on the generated key without being detected. With the above limitation of QKD in mind, there are several approaches to a proper security statement. The approach that is most commonly used in existing security proofs is to bind the probability that Alice and Bob generate bit-strings that are not equal, uniform, or private.

23) The Security Component in QKD

With Complex of many simple components, the scientists create cryptographic protocols. A single primitive is rarely used alone. A strong security definition for the primitive should reflect the security of using it within a larger application. This allows the security of a complex protocol to be based only on the security of the components and how they are put together, but not in terms of the details of the implementation. A useful approach is to consider the universal composability of cryptographic primitives. The first component is to ensure the security of a basic composition.

A security definition stated for a single execution of the primitive that still guarantees security of composition with other systems. This definition involves a description of some ideal functionality of the primitive (i.e. the ideal task the primitive should achieve). The second component is a universal composability theorem stating how a complex protocol can be

built out of secure components. It is simply a recipe on how to securely perform basic composition recursively.

24) Unconditional Security for QKD

The researchers analyze the assumptions of unconditional security of QKD by using the quantum universal composability. The setting for QKD is simpler than that considered in the past, already in 2003, Prof Ben-Or and other researchers researched the composability theory, and also the composing quantum and classical protocol. The researcher's only concern is the unconditional security and the fact that in QKD, Alice and Bob are known to be honest, and Eve is known to be adversarial, and there is no unpredicted corruption of any party. The formal corruption rules are not used in the researcher's derivation of a composable security definition for QKD. The following simplified model is sufficient for the researcher's derivation of a universal composable security definition for QKD.

25) The Quantum Circuit Model

The researchers first describe the model for quantum protocols and other concepts involved in the quantum composable security definition. The (acyclic) quantum circuit model is the basis for this subject. An acyclic circuit is a partially ordered set of gates. However, associating the circuit with constraints on the timing of the adversarial attack is a delicate issue. Suppose the circuit contains conditional gates controlled by random public classical registers. The gates on the target may or may not be applied depending on the values of the control registers – and when the gates are not applied, the associated time-constraints of the adversarial attack disappear. In the extension to the usual acyclic circuit model, the researchers consider

all possible values of the control registers and the resulting sets of nontrivial partially ordered operations, and the corresponding constraints on the adversarial attack.)

The researchers only considered circuits in the extended model.

i. Structure of a protocol a (cryptographic) protocol P can be viewed as a quantum circuit in the extended model, consisting of inputs, outputs, a set of registers, and some partially ordered operations. A protocol may consist of a number of sub-protocols and parties. Each sub-protocol consists of smaller units called "unit-roles," within each the operations are considered "local." For example, the operations and registers of each party in each sub-protocol form a unit-role. Communications between unit-roles within a sub-protocol represent internal communications; those between unit-roles in different sub-protocols represent input/output of data to the sub-protocols. A channel is modeled by an ordered pair of operations by the sender and receiver on a shared register. The channel available to perform each communication determines its security features.

ii. Security in terms of indistinguishable ideal functionality let P_I denote the ideal functionality of P. Intuitively, P is secure (in a sense defined by P_I) if P and P_I behave similarly under any adversarial attack. "Similarity" between P and P_I is modeled by a process between an environment ε and a simulator S. These are sets of registers and operations to be defined, and they are sometimes personified. In general, P and P_I have a very different internal structure and are very distinguishable, and the simulator S is added to P_I to make an extended ideal protocol P_I+S that is less distinguishable from P. ε consists of the

adversaries that act against P and an application protocol that calls P as a sub-protocol. At the beginning of the process, P or P_I+S are picked at random. ε will call and act against the chosen protocol, and will output a bit Γ at the end of the process. The similarity between P and P_I+S (or the lack of it) is captured in the statistical difference in the output bit Γ.

iii. Valid ε: The application and adversarial strategy of ε are first chosen (the same whether it is interacting with P or P_I+S). ε has to obey quantum mechanics, but is otherwise unlimited in computation power. If P is chosen in the process, ε can

(a) Control the input/output of P

(b) Attack insecure internal communication as allowed by the channel type

(c) Direct the adversarial parties to interact with the honest parties in P.

ε +P has to be an acyclic circuit in the extended model (as mentioned above).

iv. Valid P_I and S: If P_I+S are chosen in the process, ε (a) controls the input/output of P_I as before. However, the interaction given by (b) and (c) above will now occur between ε and S instead. (S is impersonating or simulating P.) The strategy of S can depend on the strategy of ε. P_I should have the same input/output structure as P, but is otherwise arbitrary. (Of course, the security definition is only useful if P_I carries the security features the researchers want to prove for P.) In particular, P_I may be defined with internal channels and adversaries different from those of P. S can (b) attack insecure internal communication of P_I

and (c) direct the adversarial parties to interact with the honest parties in P_I. Thus, P_I exchanges information with S, and this can modify the security features of P_I. To ε, S acts like part of P_I, "padding" it to look like P, while to P_I, S acts like part of ε. It is amusing to think of S as making a "man-in-the-middle" attack between ε and P_I. Finally, ε +P_I+S have to be an acyclic circuit in the extended circuit model (as mentioned above).

The symbols P and P_I+S are also used to denote the respective events of their being chosen at the beginning of the process.

26) Universal Composability Theorem

Theorem 1: Can be generalized to any arbitrary protocol with a proper modular structure. An example of an improper modular structure is one with a security deadlock, in which the securities of two components are interdependent.

Theorem 2: is obtained by recursive use of theorem 1 and the triangle inequality. The idea is to replace sub-protocols one-by-one by their ideal functionalities at the highest level, and proceed recursively to lower levels toward the root. The distinguishable advantage between P and P_I is upper bounded by the sum of all the individual distinguishable advantages between pairs of protocols before and after each replacement.

The composable security definition for QKD derived in the simplified setting will remain applicable in the general setting. However, when

applying Theorem 2 to analyze the security of an application using QKD, one should use a setting appropriate for that particular application.

27) Main Result of Prof Ben Or's protocol:

Prof Ben-Or and his associates assume pair wise quantum channels and a classical broadcast channel between any numbers of participants. They presented a universally composable, information theoretically statistically secure multiparty quantum computation protocol that can tolerate an adaptive adversary controlling up to less than half of faulty participants. The complexity of the protocol is polynomial in the number of participants and the size of the circuit.

In their setting, universally composable classical secure multiparty computation is possible. In their protocols they make extensive use of this classical cryptographic primitive. One strategy that is used extensively is to reduce the quantum multiparty computation to a secure computation on classical keys.

A verifiable secret sharing is the first step in developing a secure multiparty computation and the protocol for this is similar in structure to the classical one. There is however major obstacles that need to be overcome in the quantum case. Both protocols use authentication codes but in the quantum setting authentication require encryption and techniques must be developed to work with encrypted data. Another important difference is that in the quantum setting the distributor of the information cannot keep a copy of the input state in case there is trouble. To solve this, the protocol first generates a shared EPR pair, half held by the distributor and the other half

being shared correctly among the participants. Then the distributor can introduce the input state to the computation via teleportation.

28) Simulation

Prof Ben-Or and his associates took extra care to guarantee that their protocols will be universally composable. The protocols they present are quite involved and might not have optimal complexity. They do have one property — the simulation required for their correctness proof is simple and straightforward.

29) Secure Multiparty Quantum Computation with (only) a strict Honest Majority. (Appendix G)

In QKD the subjects of secure multiparty computation and authentication are major ones. In this research, the researchers; Prof Ben-Or and his associates examine these subjects. They analyze different aspects of these subjects and establish few different new protocols to be able to operate according to them. By new protocols they prevent the situation that Eve locates herself between Alice and Bob to get information from both sides without their awareness.

When quantum communication is established between more than two parties, some might not be honest. Prof Ben-Or and his associates also research how many parties that are in the circle of communicating must remain honest and follow the protocols in the right way to be able to transfer secret information among the honest parties.

Following are indications of some protocols which are mentioned in this research which relate to the above subjects.

A. A general security multiparty computation (MPOC)
B. The verifiable quantum secret sharing (VQSS)
C. The Weak Quantum Secret Sharing (WQSS)

According to protocols A &B, the communication among the multiparty can tolerate $\frac{n-1}{2}$ dishonest participants, n presents the number of participants.

These two protocols show a larger fraction of errors than traditional.

The research introduces new schemes of authentication and approximate codes tailored to the needs of the protocols, as well as new state purification techniques along the lines of those used in fault-tolerant quantum circuits.

The two protocols A & B, make extensive use of this classical cryptographic primitive. One strategy that is used extensively to reduce the quantum multiparty computation is to secure computation on classical keys. In fact, a verifiable secret sharing in the first step in developing a secure multiparty computation (MPC) and the protocol for this is similar in structure to the classical verifiable secret sharing. Both protocols use authentication codes but in the quantum setting authentication require encryption and it must develop techniques to work with encrypted data.

Another important difference between the classical and quantum system is that in the quantum setting the scientist found a solution to the problem that the dealer cannot keep copy of the input state in case there is trouble. The solution is half held by the dealer and the other half being shared correctly among the players. Then the dealer can introduce the input states to the computation via teleportation.

In this research, the scientists contribute in the field of quantum authentication a family of self-dual quantum authentication schemes. They built a scheme which is exponentially secure in some arbitrary security parameters.

The researchers manipulate the classical keys in many ways. They use an imaginary classical Trusted Third Party, which implements classical multiparty computation. From now on, all classical keys of authentication data will be sent to a third party who will tell the participants the meaning of their actions

The scientists in their research, in the part of verified quantum state authentication, show how to force the dealer to send to every honest participant a correctly authenticated message. The dealers send states of the form to all participants in order to authenticate them. The problem is to distinguish between an honest participant or dealer and a dishonest one. To solve this problem, the researchers incorporate the protocols which enable to catch the dishonest dealer or any participant who has a large number of (o) states authenticated by the dealer.

The researchers present all the possibilities of honest and dishonest dealer or participants and how to identify who is who.

Another protocol that Prof. Ben-Or and his associates present is The Weak Quantum Secret Sharing (WQSS). This protocol has two phases. In the first phase the dealer shares the secret among all participants such that the dishonest participant has no information about the state. In the second phase, the quantum data is sent to constructors who reconstruct the secret. In case that no state is reconstructed, the re-constructor will know that the dealer is dishonest and at the end of the sharing phase, the participants have a state encoded in the quantum error tolerant secret sharing scheme with security to know if the dealer is dishonest or not.

The Protocol Verifiable Quantum Secret Sharing (VQSS) has also the same two phases as protocol WQSS, the difference between them is the dealer capability to ruin the secret after it has been shared. The scientist solves this problem by sharing the secret using the protocol WQSS and this means that the dishonest participants no longer have control on their shares. They can eliminate their shares by causing the WQSS reconstruction to fail, but cannot change them to some other state which could spoil the dealer's original state.

30) Trust Among the Multiparty Computation

i. Secret sharing and multiparty computation allowing a group of mutually distrustful participants to perform correct, distributed computations under the sole assumption that some number of them will follow the protocol honestly.

ii. The question is how much trust is necessary – that is, how many participants must remain honest – in order for distributed quantum computations to be possible.

iii. The researchers present a verifiable quantum secret sharing (VQSS) protocol and a general secure multiparty quantum computation (MPQC) protocol.

iv. These protocols rely on approximate quantum error-correcting codes, which can tolerate a larger fraction of errors than traditional, exact codes. New families of authentication schemes are introduced here and approximate codes tailored to the needs of the protocols, as well as new state purification techniques along the lines of those used in fault-tolerant quantum circuits.

v. Authentication

Ben-Or and his associates built a family of self-dual Quantum Authentication Schemes which was based on the quantum authentication scheme that was proposed by Howard Barnum, and his associates in their "Authentication of Quantum Messages," in 2002. They stated that any Quantum Authentication Scheme based on a quantum CSS code can be used, but they proved that using their self-dual code is simpler. The proof is enclosed in Appendix D.

31) The New Protocol for Multipart Quantum Computation

A secure quantum multiparty protocol allows any number of participants to compute any number of input quantum circuits where each participant is responsible for providing one of the input states. The output of the circuit is broken into a number of components and each participant receives the output. Note that the inputs are arbitrary (possibly entangled) quantum states and each participant simply has his input in his possession — he does not need to know the classical description of it. Informally, the wish is to achieve the same functionality as if each participant were to hand his input to a trusted third party who would evaluate the circuit and distribute the outputs, even when some participants are faulty.

At first the best situation would be that the faulty number of participants tolerated would be smaller than a quarter of all participants. Simply because (exact) quantum error correcting codes (QECC) cannot recover from more errors. Indeed, the best previously known verifiable quantum secret sharing protocol can tolerate the faulty number of participants to be smaller than a quarter of all participants, and the best

secure quantum multiparty protocol can operate only when dividing the number of faulty participants to 6. In fact, some researchers determine that approximate QECCs exist that can recover (with high probability) from the corruption of more than half faulty participants. This discovery paved the way to the protocol of Prof Ben-Or.

32) General Security Definition and Composability for Quantum & Classical Protocols. (Appendix F)

Prof Michael Ben-Or from the Hebrew University, Jerusalem and his associate Professor Dominic Mayers from, IQI, California Institute of Technology, researched the "General Security Definition and Composability for Quantum & Classical Protocols."

The scientists adopted the classical model as Canetti defined it, to the quantum model by building a new model depending on the previous results.

The researchers unfold the basic principle that was set up by Canetti whose definition states that the sub-protocol can be replaced with an associated ideal protocol together with a simulator, and the environment of the protocol will not notice the difference. The researchers presented a different model that is more adapted to quantum protocols.

The researchers unfold the universal composability theorem which was first reported by D. Mayers and M. Ben-Or in their article "Composing Quantum and Classical protocols" which was presented at the Quantum Information Processing in December 2002.

The protocol in their research model as in the classical case, must also define environments, ideal protocols and simulators.

The target of this research is to introduce the more structured framework of universal composability in the quantum world. The researchers give an example of the difficulties that arise in the unrestricted framework but it will never replace the understanding that many researchers gained through the experience of proving or trying to prove the security of complex protocols. The universal composability framework is a practical framework that allows security results that seem otherwise difficult to achieve.

To summarize the research, its contribution is to unfold the framework of universal composability in a model that is well adapted to quantum protocols. It is also an interesting alternative model for the universal composability of classical protocols as well.

In this research the researchers discuss examples of the five main concepts, the concepts of protocol, application, adversary, ideal protocol and simulator, and give the ideas that are crucial in the composability theorem.

The researchers used the idea that the universally composable theorem of Canetti is also valid in the quantum world.

To give an example that is all classical but will be enough to explain the basic idea, see the example in the research clause No. 2.1 which includes a bit of commitment from Alice to Bob and from Bob to Alice and also can

be constructed with the help of a trusted party, who is called Charlie. This protocol is formally defined in Appendix B of this research.

The researchers deal in this work in application protocols which deals with adversary circuits. The application is a set of role-circuits that provides inputs to the bit commitment protocol and receive outputs from this bit commitment protocol. The application can also communicate with the adversary circuits that are active. The application together with the adversary is called the environment.

33) Quantum Circuits with Mixed States (Appendix H)

Dr. Aharonov, Dr. Kitaev and Dr. Nisan generalized the formal model of quantum circuits. They generalize the formal model of quantum circuits, a model in which the state can be a general quantum state, namely a mixed state, or a "Density Matrix", and the gates can be general quantum operations, not necessarily unitary.

The new model is equivalent in computational power to the standard one but it solves some of the central issues like: measurements in the middle of the computation de-coherence and noise using probabilistic subroutines, and more.

The main result, in this research, is a solution for the subroutine problem. It defines a natural notion of using general subroutines and shows that using general subroutines does not strengthen the model. The researchers prove a simple lower bound on depth of circuits that compute

probabilistic findings. They use the so called "Trace Matrix" on density matrix to show how to keep track of errors in the new model.

This work defines quantum circuit which is allowed to be in general quantum states, i.e., a mixed state, and which is allowed to use any quantum operation as a gate not necessarily unitary.

The problems that are solved by this work are:

i. It becomes possible to allow measurements in the middle of computation.
ii. Noise and de-coherence are key obstacles in implementing quantum computer devices. This work gives solution to these problems.

The main technical result of this work is a solution of one more problem in unitary model, namely the subroutine problem.

The researchers were able to give a natural definition which generates both, the case of deterministic subroutines on super positions and the case of probabilistic subroutines on classical input. The research gives all definitions and proofs using the density matrix picture.

The bottom line is: The research provides the physical background in the mathematical language which defines the model and provides basic theorem regarding the model which includes an example of complexity bound using density matrix.

34) Quantum Key Distribution by Free Space MIMO System, By Dr. Motty Gabay and Dr. Shlomi Arnon. (Appendix I)

In order to provide high security transmission, the researchers propose the QKD bit rate using a communication system that includes a multiple-input multiple-output quantum key distribution (MQKD). Such a system can enable a number of receivers to communicate simultaneously with a number of transmitter elements which consequently increases the overall QKD bit rate.

The researchers present, due to scattering and turbulence in the atmospheric channel, a method which may introduce interference effects that reduce the system bit rate and increase the quantum bit error rate.

The researchers present a model for analyzing the effect of crosstalk and interference on the MQKD.

They found that atmospheric effects impair performance. In order to mitigate the atmospheric effect using several wavelengths simultaneously, they also give criteria to define the number of wavelengths that are required to achieve a given performance.

The researchers claim that due to simultaneously communication of both transmitter and receiver in the system, the overall QKD bit rate is increased but will still be limited due to atmospheric effects such as the absorption aerosol scattering and turbulence. Multi-scattering and turbulence could deflect the photons to directions other than their original destination,

which can cause the deflected photons to miss the appropriate receiver element, or even to reach the wrong receiver element.

The solutions for these disturbances are impaired performance including low bit rates and high quantum bit error rate (QBER).

The researchers suggested using several wavelengths simultaneously. They provide criteria to define the number of wavelengths that are required to achieve a given performance.

They show how several wavelengths can reduce crosstalk and interference and provide criteria to define the number of wavelengths that are required to achieve a given performance, but still due to atmospheric effects, some of the photons may deflect and create errors in the original and neighboring detectors. As a result, the quantum bit error rate increases and the data rate decreases. The proposed option is to use several wavelengths in the system in order to improve the bit rate. If each transmitter-receiver couple will use a different wavelength, each receiver can filter all the stray photons that it receives and collect only the photons that were intended for him.

In this research, the researchers showed a mathematical method for analyzing the BB84 protocol over a MQKD system, which includes an array of QKD transmitters and receivers. This method provides approximate results due to the averaging means of the optical transfer function. The atmospheric effects were shown on the system's performance and the decrease of the performance as the distance between Alice and Bob

increases. This shows the improvement of the quantum bit error rate as the number of wavelengths was increased.

4. Sales Situation for Quantum Key Distribution.

Up until today, Israel's researchers are still in the R&D stage. This is due to the fact that all the developments for a working quantum cryptographic system still do not give a good performance. The researchers advise that a good working system will still take time to be developed into a working device that will be sold and marketed in the local or overseas markets. This is due to the need for more research and the fact that the classical systems which are in the market today still serve the security needs. This situation will be stable until the quantum computer will enter the market.

5. Export Control

Engagement in Encryption Items in Israel is controlled under the Law Governing the Control of Commodities and Services from 1957, which was legislated for purposes of law enforcement and the protecting of Israel's national security. The Policy aims to balance between national security interests on the one hand and preserving competitive Hi-tech Industry on the other, whilst enabling users to engage in encryption without over-burdening restrictions.

Following the 1998 amendment of the "Encryption Order" - which, amongst others, transferred the authority of Control and Licensing to the Director General of the Ministry of Defense (IMOD) - The Commercial Encryption Items Export Controls Policy was updated in 1999. Further to updating the Export Policy and in order to facilitate and assist the Israeli Encryption Industry and users of Encryption Items in the fields of

development, manufacture and sales, it was decided to update Israel's Policy of Engagement in Commercial Encryption Items within Israel.

A person is exempted from applying for a license for Engagement in Commercial Encryption Items subject to the following conditions:

i. The product or Encryption Items was purchased from a license holder for sale and distribution of Commercial Encryption Items.
ii. The product or Encryption Item was "Downloaded" from the Internet for personal use for Data Security or Electronic Signature.
iii. The "Certification Authority", as defined in the Electronic Signature Bill of 2000, authorized under law to issue Electronic Signatures: will be exempt from receiving a License for Engagement in Encryption if the Encryption Item is purchased from a license holder.

Should the "Certification Authority" request to import, independently, Encryption Items for Electronic Signature, it is authorized to do so prior to receiving a license, subject to the following conditions:

i. Immediate notification of the Ministry of Defense upon the beginning of the use of the Encryption Items.
ii. Submission of application for a License for Engagement in Encryption Items, including required technical documentation.
iii. Submission of Encryption Items for technical review according to the Ministry of Defense requirements.

With regard to financial institutions supervised by the State (such as banks and insurance companies), the Advisory Committee to the Director-

General of IMOD is reviewing additional reforms in the licensing process similar to those granted to the "Certification Authorities".

1) Sales of encryption goods

In the event of a request by a foreign company wishing to sell Encryption Items directly to users in Israel (without a distributor or local representative), the company representative or a person empowered by it will be given a License for Selling and Distributing, following the product's technical review.

2) Export of encryption goods

Subject to the provisions of the Encryption Order, including the obligation to submit a license application to engage in Encryption Items and have the IMOD scrutinize the said application, the applicants shall be granted a license to export commercial encryption items, without limiting the key length, to all non-governmental end users in most countries world-wide. For some countries, the license shall also be valid regarding governmental end users.

- Licenses shall not be granted for the export of encryption items to a small number of countries.
- Those engaged in the export of encryption items shall still be obligated to report to the IMOD.
- Export licenses for encryption items shall be granted after scrutiny by the IMOD, and the license will have to be renewed on an annual basis.

6. Single Photon Source

When the concept of the photon was first used, the single photon was not considered. Until the ideas and methods of quantum optics were used, the “single-photon” weakened a laser beam to ensure that the probability of having more than one photon became negligible. However, such weakened beams differ from “true” single photons in at least two aspects: first, the vacuum probability is much higher than the probability of detecting a photon, so one gets a “no-photon” with occasional detection of a photon; second, the probability of getting two photons is never zero.

Although the weak beam has been useful in quantum optics, the appearance of quantum information science has placed limited demands on optical sources, those sources produce single photons either on demand or when called for. In particular, secure quantum cryptography and linear optical quantum computing depend on the availability of such single-photon sources.

The focus on QKD recognizes that single-photon sources need development and presents researches covering the spectrum of activity in the field.

Photon detection performs a critical role in assessing single-photon sources as well as advising of the arrival of a single photon.

The quantum dot is so small that it can at most capture a few electrons and holes from a pulse of electric current. A single photon is created by the recombination of a single electron and a single hole in the dot.

The researchers believe this is the first electrically driven single-photon source. Such single-particle-emitting sources are essential for a truly secure form of quantum cryptography. Otherwise, if several photons spill out from a device at a time, the extra ones can be directed off by an eavesdropper, who could then forward a message without being detected.

One of the largest challenges for building quantum communications networks involves having single photons, which are needed to ensure the security and efficiency of quantum systems. With an adequate supply of single photons, quantum communications systems could send information at nearly the speed of light, compared with the electron speed and resistance in classical systems

Several technological and theoretical barriers still have to be overcome to improve the performance of current QKD systems. Most of them rely on Weak Coherent Pulses (WCPs) as an approximation to single photons. Such classical states are very simple to produce, but a fraction of them will contain two photons or more. Since information exchanges using such multiphotonic pulses can be spied on by potential eavesdropping strategies, security hazard is introduced into the key distribution process. For QKD schemes relying on WCP, the people communicating need to throw away at the end a part of the initially exchanged information, in proportion to what an eavesdropper could have learnt from it. Indeed, in WCPs' schemes, the probability for multiphotonic pulses is directly connected to the mean intensity of the initial pulse that must therefore be weakened more and more to guarantee security as line losses become higher. Therefore, either the transmission rate at long distance becomes vanishingly small or complete security cannot be guaranteed.

The use of a true Single-Photon Source (SPS) has a great advantage over WCPs' schemes since it potentially permits greater per-bit extraction of secure information. This advantage becomes significant for systems having high losses on the quantum transmission channel such as the envisioned satellite QKD. Single-photon quantum cryptography has been implemented in several experiments, which gave clear evidence for the advantages of SPS.

It is compulsory to send pulses of only one photon. This is because if a pulse sent by Alice with more than one photon is detected by Eve in the wrong base, it may give a count in two of Eve's detectors; this tells Eve that she used the wrong base. She can then simply discard this transmission. However, when she receives only one photon, Eve has no other choice but to send the photon to Bob in the same state in which she measured it. This will create errors in the string received by Bob. These errors in the key will indicate Eve's presence to Bob and Alice.

7. Performance

1) Two Color Parametric Down Conversion

By Dr. Tal Mor and Dr. Meir Orenstein (Appendix K)

The Technion researchers researched the single photon source usage. This research was done to find out if a single photon will expand the security for quantum key distribution.

The main task was to securely transfer secret information between two honest parties, Alice and Bob without revealing it to Eve. This research comes to check how to overcome the Photon Number Splitting Attack (PNS) which Eve can use when security is limited due to the usage of weak coherent pulses for single photon source. This approach limits the security level. In this case Eve can measure each pulse sent by Alice. She blocks part or all the pulses that contain one photon. If more than one photon is found, she keeps one photon in a quantum memory and sends the rest through a lossless fiber to Bob. As the lossless fiber imitates the original rate, she will not be revealed due to a different rate. At this stage, she will wait to receive through the classical channel the basis that Bob measured the received photons and by this she will have the key between Alice and Bob.

In order to obtain better security, against the Photon Number Splitting Attack, quantum cryptographic applications, teleportation and quantum computation photon pairs of Spontaneous Parametric Down Conversion (SPDC) can be used. Which means, counting the number of photons at

Alice's side, (she is the idler), whenever only one photon is detected, this single photon will be sent to Bob.

The idler is fed through a bandpass filter centered at 770nm to a photon counter based on Si detector. Whenever exactly one photon is counted, the electro-optic shutter is opened and the correlated photon is sent through a bandpass filter centered at 1550 nm via a long filter to Bob. On Bob's side, there is an InGaAs detector which is used to resolve single photons. The Si counter and the InGaAs detector are synchronized in order to signal the InGaAs detector about the coming photon.

Research results

The researchers suggested an experimental channel scheme based on theoretical idea of a two color type I-SPDC source. They were looking for new options to improve security against Photon Number Splitting Attacks.

2) Effect of Turbulence on Quantum Key Distribution Scheme Based on Transformation from the Polarization to the Time Domain Laboratory Experiment

Research by Dr. Motti Gabay & Dr. Shlomi Arnon (Appendix K)

This research comes to show that there is no need for many detectors when transforming polarization states to time slots. The researchers came up with a system that will simplify the architecture and reliability of the system including making it lighter in weight. These applications will be important in the future of quantum communication which will be used in airplanes and satellites.

Bennett was first to use polarization coding systems, he used one detector and two polarization rotators. He transmitted faint light pulses, containing less then one photon on average, which was produced by a LED. Then Hughes used a polarization coding setup, which operated over a 10-km range, both in daylight and at night. In his setup, four detectors were used, one for each polarization state.

Bennett also first encoded the value of Q-bits with the phase of photons. In his method, he used two Mach-Zender interferometers and one detector. The use of only one detector was made possible by the introduction of time delays in the optic path, which lead to temporal separation of the received photons. It was difficult to keep the transmitter and the receiver's interferometers stable within a fraction of a wavelength of the photon during the key exchange. For long key exchanges, an active system is necessary to compensate for the drifts.

In this research, the researchers propose two polarization coding systems which do not need active polarization modules, and still have only one detector. This is achieved by mapping the output of the individual polarization base states onto unique time slots.

The new schemes they developed are simplified implementations of the QKD BB84 protocol, and the QKD B92 protocol.

As proved in BB84 after Alice and Bob will create the QKD and after they complete the full QKD procedure, they will have the same cryptographic key and they can start transmitting secret information knowing that they have full security. Also due to the no-cloning theorem, they know that Eve will not be able to copy a quantum system in an un-known state. Alice and Bob will also need to predict Eve's possible strategies.

If Alice and Bob send pulses of only one photon, it will be impossible for Eve to detect the base in order to measure it. She will have no choice but to send the one photon she received to Bob in the same state she measured it. As if more than one photon is sent from Alice to Bob, it may give Eve an advantage of knowing the base of the transmission, she will be able to measure the transmitted information with instruments similar to Bob's and resend similar pulses to Bob, and by that she would know the shared bits by Alice and Bob.

The Researchers' New Scheme for Implementing the BB84 Protocol

The researchers suggest using the BB84 protocol with the following changes:

Alice will encode a random key by using a four laser diodes. Each diode transmits a photon with different polarization using four polarizers. Bob uses polarized beam-splitters to separate the polarizations, and four different time delays to distinguish between them. Alice's transmitter transmits simultaneously a single photon in the chosen polarization state and a gate pulse to Bob. A photon entering Bob's receiver encounters a 50/50 beam-splitter and randomly decides which path to follow. Each path represents a different base, one for -45 deg/ +45 deg and another for 0 deg and +90 deg. Each path uses a polarized beam-splitter to distinguish between 0 and 1 and has a different optical delay for each polarization angle (a total of four different delays). All paths end at the same photon detector. Another detector is used to detect the gate pulses. Since photons with different polarizations are received with different delays, the photon's delay from the gate pulse will reveal which polarization angle was detected. This design enables to use just one photon detector to distinguish between four different polarizations instead of four photon detectors. And there are no moving parts in this design, which makes the system simple to implement and maintain.

The Researchers' New Scheme for Implementing the B92 Protocol

In this scheme, the researchers suggest that Alice will use two laser diodes to encode a random key. Each diode transmits a photon with a different polarization. Bob uses a 50/50 beam-splitter to randomly decide which measurement to make. Each path from the beam-splitter then uses a polarized beam-splitter to distinguish between polarizations, and therefore

two different optical delays are generated. The two paths end at the same photon detector.

In order to differentiate between polarizations, the researchers suggest using delays in transmitting the photons which will reduce the maximum bit rate of the system.

In order to determine the delays, there are several issues that need to be considered:

i. The time slots for the polarization decision pulses, each declared by the gate pulses, must not overlap. This means that the shortest delay must be longer than the gate pulse duration and the longest delay must be less than the frame time, at the end of which the next gate pulse will arrive.

ii. The delays must be different from one another, otherwise, it will not be possible to differentiate between different polarizations.

iii. The electronic time response must be taken into account.

iv. The single photon detector must have adequate recovery time to redetect photons in the subsequent time slot. Otherwise, in the case when two photon signals arrive at the same time, the detector will not acknowledge the second and will not realize that the signal is contaminated. The arrival of two or more photons means that stray undesired photons arrived, or that deliberate interference contaminated the signal. Consequently, this event should be discarded.

Turbulence

Turbulence can affect the performance of free-space QKD systems due to atmospheric changes. Turbulence effects occur at all altitudes but are stronger in the lower atmosphere.

The researchers in this research created an artificial turbulence by locally heating the air along the propagation path. The temperature of the heated air was used as a measure of turbulence strength, and the communication performance was investigated as a function of this metric.

The Experiment

The Researchers set up an experiment in order to implement the B92 Protocol. They set up a system where Alice starts the QKD by pulsing the diode lasers, and Bob's receiver's kHz is reduced. They use a temperature-controlled heating element to produce turbulence effects at different levels corresponding to locally heated temperatures. They measured the turbulence effect on the code generation rate.

Conclusions to the Experiment

The researchers manage to present a new design for simplifying the implementation of the QKD BB84 protocol and the B92 protocol and to reduce the number of detectors.

They manage to reduce the payload which will be important for future mobile quantum systems such as satellites and airplanes, where lightweight and compact hardware is needed.

8. Sales Situation for Single Photon Source

The sales situation in the single photon source is also still in the R&D stage. Many researchers are still waiting to be able to produce a system that will absolutely control the single photon on high levels. All the leading Universities and Institutes are still researching this issue hoping to find the solution to this problem.

9. Summarization

The needs for advanced technology to protect and defend the security of countries, the systems of companies and people's privacy is behind the reason to keep looking to develop new technologies in the field of communication.

The classical systems that are used today to secure communication between people are not enough. Great efforts and huge amounts of money are invested to develop the classical system but still these systems's security can not proven.

The first step which was taken by Bennet Brassard in 1984 (BB84) to develop a new system based on quantum proved security in a manner that will be able to replace the classical system.

Even though huge advance has been done since the 1984, having a complete system is still far away. It seems today that the researchers need more than one decade to complete a working system for QKD. One of the main issues that its development still needs to be completed is the quantum computer which will enhance the quantum technology. Another issue that is still being developed is an ideal single photon source. Even though some technology is used in the world of encryption, still this technology needs to be developed.

The researchers are focusing on more effective and faster photon detector.

The goal is to make quantum cryptography more useful and reliable integrated with today's telecommunication infrastructure and increase the transmission distance.

Quantum research is also taken to many additional applications and fields like, medical fields, complicated sensors, electronics, different defense devices, navigation systems, precise watches and more. It seems that the quantum technology will replace many of the classical technologies that are known today and in the future the quantum technology will become part of our daily life.

10. Reference List

A. Aharonov Dorit and associates, June 2006, Quantum Circuits with Mixed States.

B. Aharonov Yakir and Vaidman Lev, 1996, Protective Measurements of Two State Vectors.

C. Ben Kish and Associates, May 26th 2006, Quantum Control, Quantum information Processing and Quantum-limited Metrology with Trapped Ions.

D. Ben-Or Michael and Associates, April 11th 2006, Security Multiparty Quantum Computation with (Only) Strict Honest Majority.

E. Ben-Or Michael, June 25th 2006, The Universal Composable Security of Quantum Key Distribution.

F. Ben-Or Michael and Mayers Dominic, Nov. 2004, General Security Definition and Composability for Quantum & Classical Protocols.

G. Biham Eli, Mor Tal and associates, Algorithmica, 2002, Security of Quantum Key Distribution against All Collective Attacks.

H. Biham Eli, Mor Tal and associates, April 24th 2006, A Proof of the Security of Quantum Key Distribution, Journal of Cryptology.

I. Gabay Motty and Arnon Shlomi, April 2005, Effect of Turbulence on a Quantum-Key Distribution Scheme Based on Transformation from the Polarization to the Time Domain: Laboratory Experiment.

J. Gershoni D and associates, 2006, Magneto Optics of Single Photons emitted from Single InAs/GaAs self-assembled quantum dots in a planar microcavity.

K. Gershoni D and associates, 2006, Emission Characteristics of Quantum Dots in Planar Micro Cavities.

L. Mor Tal and Izmely Oleg, July 29th 2006, Chosen Ciphertext Attacks on Lattice-Based Public Key Encryption and Modern (Non-Quantum) Cryptography in a quantum Environment.
M. Mor Tal and Associates, 2006, Two-Color Parametric Down Conversion.
N. Mor Tal, and associates, 1996, Parity Bit in Quantum Cryptography,
O. Mor Tal and associates, 1995, Quantum Cryptography with Coherent States.
P. Vaidman Lev and Kalev Amir, 2005, Measurement of an Integral of a Classical Field with a Single Quantum Particle.

11. Appendix List

A. A Proof of the Security of Quantum Key Distribution, Journal of Cryptology, April 24th 2006, by Prof Eli Biham and Dr. Dr. Tal Mor and associates.

B. Chosen Ciphertext Attacks on Lattice-Based Public Key Encryption and Modern (Non-Quantum) Cryptography in a quantum Environment, July 29th 2006, by Dr. Tal Mor and Oleg Izmely.

C. Security of Quantum Key Distribution against All Collective Attacks, Algorithmica, 2002, by Prof. Eli Biham and Dr. Tal Mor and associates.

D. The Hand Written proof of Security of BB84 QKD Protocol by Michael Ben-Or

E. The Universal Composable Security of Quantum Key Distribution, June 25th 2006, by Michael Ben-Or and associates.

F. Secure Multiparty Quantum Computation with (Only) Strict Honest Majority, April 11th 2006, by Prof. Michael Ben-Or and Associates.

G. General Security Definition and Composability for Quantum & Classical Protocols, Nov. 2004, by Michael Ben-Or and Dominic Mayers.

H. Quantum Circuits with Mixed States, June 2006, by Dorit Aharonov and associates.

I. Quantum Key Distribution by Free-Space MIMO System, August 2006, by Dr. Motty Gabay and Dr. Shlomi Arnon.

J. Two-Color Parametric down Conversion, 2006, by Tal Mor and associates.

K. Effect of Turbulence on a Quantum-Key Distribution Scheme Based on Transformation from the Polarization to the Time Domain: Laboratory Experiment, April 2005, by Dr. Motty Gabay and Dr. Shlomi Arnon.