From classical cryptography to quantum physics through quantum cryptography

Jozef Gruska

Abstract | The first goal of the paper is point out and to demonstrate large importance security issues (in a very broad sense) have for modern science, technology and society and to discuss briefly the main areas, problems and challenges of classical cryptography. Second goal is to survey some of the main problems, directions and challenges of quantum cryptography. The last goal is to review some of the main impacts the outcomes of quantum cryptography have for our understanding of quantum physics.

Faculty of informatics, Masaryk University, Botanická 68a, 60200 Brno, Czech Republik
gruska@fi.muni.cz

Keywords: quantum cryptography, cryptographic protocols, foundations of quantum mechanics

1. Introduction

Quantum cryptography, as an area of science and technology, should be seen both as a way to develop a new, and more adequate, theory of broadly understood cryptography (including a variety of issues related to security, secrecy, anonymity, privacy and trust) and as an area developing new cryptographic tools and technologies. Quantum cryptography should be also seen as a new way to get a deeper insight into the quantum world and into the potentials of post-quantum non-signaling theories.

Goals of quantum cryptography have been very ambitious. Indeed, some protocols of quantum cryptography provably achieve so-called unconditional secrecy, a synonym for absolute secrecy, also in the presence of eavesdroppers endowed with unlimited computational power and limited only by the laws of nature, or even only by foreseeable laws of nature not contradicting the non-signaling principle of relativity.

Quantum cryptography, in a broad sense, should also be seen as an area of science that introduces, develops and explores new paradigms, concepts, methods and tools to exploit the (quantum) physical world.

Development of a better, or even unconditional, security providing technologies, for generation of the classical shared random keys, has been the original goal of quantum cryptography. Its implications and contributions to the study and understanding of the quantum world are recent, unexpected, important and deep.

The search for basic concepts, tools, methods, laws and limitations of security of information storage and transmission can and should be actually seen as an important driving force of the theory and practice of the classical and also quantum information processing and communication.

2. Role, areas and approaches of modern classical cryptography

As discussed in details in [1], the history of mankind can be seen as being divided into three eras: Neolithic era, industrial era and current information era. In the neolithic era the driving force was a need to make sure that mankind has enough of *food* and whenever needed; in the industrial era the issue was *energy* instead of food and in information era it

is *information*. There are good reasons to assume that next era could be characterized similarly with *security* being of the main concern.

2.1. *Security as a new superparadigm for science and technology*

Concerning the theory of classical information processing and communication, it has been know already for quite a while that some of the most basic cryptographic concepts play the key role in the development of computational and communication complexity. This has been recently extended to the theory of formal (information processing) systems and related languages for reasoning.

Concerning information processing and communication technologies, one can also say that security concerns and needs are, beyond proper functionality and efficiency, one of the key issues influencing development of modern technologies.

One can even see that in a similar way as information processing super-paradigm has been perhaps the main super-paradigm of modern science and technology, that this role starts to played also, and perhaps even more, by the security super-paradigm.

2.2. *Could security challenges be deeper than those of efficiency?*

A natural modification of the above question is: why could security super-paradigm provide a stronger driving force for science and technology than that of information processing?

The answer is simple. The very basic requirement concerning security is perfect security, in some reasonable sense, and that requires to go deeper into the scientific understanding of the issues, and is also more demanding concerning technology designs, than the tasks to design more efficient information processing systems. The reason behind is that perfect security is often not only an extreme and an idealisation, but actually a basic necessity because weaker requirements are not of too much interest and usefulness. A nice illustrating example is that of the RSA cryptosystem.[1] Would we have a method to determine the least significant bit of the plaintext from the cryptotext, we would have method to break the RSA completely—that is security has to be in the RSA case up to a single bit. Another surprising result shows that 1 bit of information can help the eavesdropper to obtain (to unlock) in some cases an arbitrary large amount of information [2].

2.3. *Basic approaches to modern cryptography and security*

History of cryptography is thousands year old and full of fascinating stories. Modern cryptography has three sound approaches: (a) Information theory based approach—the enemy should have not enough information to break a cryptosystem; (b) Complexity theory approach—the enemy should have not enough computational power to break a cryptosystem; (c) Quantum physics approach—the enemy would need to break some laws of nature to break a cryptosystem.

Our understanding of the main types of (sufficiently) perfect secrecy has also developed much. We have: (a) Perfect (information or Shannon) secrecy; (b) Secrecy computationally indistinguishable from perfect secrecy using classical computers; (c) Unconditional secrecy ensured by physical laws.

As new recent approaches to secrecy we have: (a) Entropic secrecy—as a relaxation of information secrecy [3]; (b) Secrecy computationally indistinguishable from perfect secrecy using quantum computers (or even using tools not contradicting potential non-signaling theories); (c) universally (composable) secrecy for protocols—to be discussed later.

Much has also developed an understanding that to achieve security, and related issues, in practice is an unusually complex and difficult task. A perfection of basic algorithms and protocols is a necessary, but actually only a small issue. Technology, (side) channels and people involved play important roles and a variety, as well as sophistication, of attacks and hacking is enormous. Moreover, it has recently emerged an insight that exploration of these issues is also of a deep theoretical importance for our understanding of the information processing and physical worlds.

2.4. *Main tasks of modern cryptography*

Main tasks of current cryptography are: (a) Secrecy of the (transmitted) data (messages)—so that only the intended receiver finds the original message; (b) Integrity of the transmitted data—so that any unauthorized change of the data can be detected; (c) Signing of the digital data—digital signatures; (d) Authentication/identification—of

[1] Chosen are large primes p and q, as well as integers e, d such that $ed \equiv 1 (\mathrm{mod}\,(p-1)(q-1))$. The public key is: $n = pq, e$, the secret key is p, q, d. Encryption of the plaintext w: $c = w^e \bmod n$; decryption of the cryptotext c: $w = c^d \bmod n$.

the communicating parties and channels. (e) Non-repudiation of activities—a communicating party should not be able to convince others that (s)he did not do what (s)he did; (f) Anonymity—of the transmitter or the receiver—as the secrecy of identity; (g) Secrecy—of the input data at distributed multi-parties computing. (h) Privacy—of the individuals participating at some information processing processes; (i) Trust—a confidence of the possibility/ability of actions/management.

All these tasks have large number of variations and their practical realisation may require creation of huge systems and also industries - as it has been with digital signatures.

There are also many other important cryptographic tasks in which participants do not trust each other: e-money, e-business, e-voting, on-line auctions, contract signing, trust negotiation and so on.

2.5. *Key areas, resources and primitives of cryptography*

Main areas of modern cryptography are: secret random key distribution/generation; secret-key encryptions (one-time pad cryptosystem; Vigenere cryptosystem; DES, AES and so on); public-key encryptions (RSA, elliptic curves cryptosystem and so on); digital signatures; authentication (of communicating parties and transmitted messages); information hiding (steganography and watermarking), (classical or quantum) secret sharing, anonymity, privacy and trust.

Main primitives of cryptography are: *encryption systems*, *one-way and trapdoor functions* and predicates[2] , *hard-core predicates*[3], *randomness extractors*[4], *hash-functions*, *universal sets of hash functions*, *pseudo-random generators* and *zero-knowledge protocols* as well as basic primitives of cryptographic protocols (to be discussed below).

Randomness is an important resource of the classical cryptography. *Entanglement, non-locality* and, very surprisingly, also *noisy channels*, are powerful resources of quantum cryptography.

2.6. *Primitives of cryptographic protocols*

Cryptographic protocols are algorithms for two or more parties how to conduct communication/cooperation in such a way that certain cryptographic goals are achieved (security, secrecy, anonymity, privacy, trust ...)—even if a certain number of parties are malicious (may cheat). *Oblivious transfer, 1-out-of-2 oblivious transfer, bit commitment* and *coin-tossing* are the main primitives of cryptographic protocols.[5] Using a secure oblivious transfer protocol one can implement a secure bit commitment protocol and using a bit commitment protocol one can implement a secure coin-tossing protocol. Using oblivious transfer one can implement securely any multiparty computation at which each party keeps secret its inputs.

Basic primitives of quantum cryptography are: quantum one-time pad and its generalisations via private channels and randomization, quantum variations on coin tossing, bit commitment and oblivious transfer protocols, quantum variations on zero-knowledge protocols, quantum identification and authentication protocols, quantum protocols to share and hide classical and quantum information and quantum anonymity protocols [3].

Very important are also so-called *zero-knowledge proof protocols*. A *zero-knowledge proof* of a theorem T is an interactive proof protocol for communication between a *Prover* and a *Verifier*, in which the *Prover* is able to convince Verifier, by overwhelming statistical evidence, that T is true, if it is so, but in doing that *Verifier* learns *nothing* from the interaction with the Prover beyond the validity of T. Several variants of zero-knowledge proofs differ in the way the notion of *learning nothing* is formalized and how many (non-cooperating provers) are involved [3].

2.7. *Modern approaches to perfect security of cryptosystems*

The problem how to define perfect security is very complex and, in a way, in the heart of the theory

[2] A function $f : \{0,1\}* \to \{0,1\}^*$ is one-way if (a) f is easy (in polynomial time) to compute; (b) there are $c, \varepsilon > 0$ such that $|x|^{\varepsilon} \leq |f(x)| \leq |x|^{c}$; (c) For every randomized polynomial time algorithm $\mathcal{A}$ and any $c > 0$ there exists an N such that for any $n > N$, $\Pr(\mathcal{A}(f(x)) \in f^{-1}(f(x)) \leq \frac{1}{n^c}$.

[3] A predicate $p(x)$ is a hard-core predicate for a function $f(x)$ if $p(x)$ is easy to compute given x, but very hard to predict given $f(x)$ (that is with probability larger than $1/2$).

[4] Extractors extracts almost uniform randomness from an imperfect source of randomness with the help of an independent uniform seed.

[5] In a coin-tossing protocol two distant and not trusting each other parties toss a random coin; in a bit commitment protocol a party A commits itself (in the so-called *commit phase*), for a party B to a bit b in such a way that B has no way to learn b, the party A has no way to change the commitment once it was made, but can convince B about his/her commitment (in the so-called *opening phase*) if needed; in a 1-out-of-2 oblivious transfer protocol a party A can send two messages to a party B in such a way that B can choose which message receives, but A will have no information what B has received.

of modern cryptography. To illustrate modern approaches to this problem let us discuss, at least briefly, the main attempt to define perfect security for classical encryptions [4]

Definition 1 – semantic security of encryption. A cryptographic system with encryption function e is *semantically secure* if for every feasible (polynomial time randomized) algorithm A, there exists a feasible algorithm B so that for every two functions

$$f, h : \{0,1\}^* \to \{0,1\}^n$$

and all probability ensembles $\{X_n\}_{n\in\mathbf{N}}$, where X_n ranges over $\{0,1\}^n$,

$$\begin{aligned}\Pr[A(e(X_n), h(X_n)) &= f(X_n)] \\ &\neq \Pr[B(h(X_n)) \\ &= f(X_n)] \leq \mu(n),\end{aligned}$$

where μ is a *negligible function.*[6]

This is a computational security approach; it limits adversaries to a probabilistic polynomial time machine.

It can be shown that any *semantically secure public-key cryptosystem* must use a *randomized encryption algorithm*

For example, as already mentioned, the RSA cryptosystem is not secure in the above sense. However, randomized versions of RSA are semantically secure.

In the case of cryptographic protocols new circumstances come into considerations when security is considered. This is mainly due to the following fact that cryptographic protocols are often used in complex environments like internet. However, they are usually originally designed as stand-alone protocols, and not as the ones to be run concurrently with other protocols.

Formal security definitions for composability use *simulation paradigm* invented to define zero-knowledge protocols. Simulation-based security requires that for any adversary attacking the real protocol there exists a *simulator* in the ideal setting, i.e. where the players only have black-box access to an ideal functionality, such that environment cannot distinguish between the real and the ideal setting.

Composability is especially tricky issue in the case of quantum protocols. One of the reasons for that is the fact that parties can postpone quantum measurements.

3. Post-quantum classical cryptography

The overall goal of post-quantum cryptography is to deal with problems that would arise when powerful quantum computers would be available. Since already nowadays some data should be kept secret for almost 100 years and powerful quantum computers may be available by that time, it starts to be important and interesting to deal with such problems.

There are four specific goals of post-quantum cryptography. The first one is to design classical secret-key cryptosystems that are secure also in the case an eavesdropper has a quantum computer to her disposal. Second goal is to find out which of the classical secret-key cryptography systems are secure against a classical eavesdropper, but not against an eavesdropper with full (or restricted) quantum artillery. The third goal is to develop and study classical public-key cryptosystems that would withstand attacks by eavesdroppers equipped with quantum computers. The third goal is to investigate in which cases classical multiparty protocols performance can change radically if some parties honestly perform the protocol, but, in addition, they share some inherently quantum resources as entanglement.

Concerning the first goal, one particular and quite urgent task is to design encryption and digital signature systems that would be both efficient enough and not breakable using quantum computers. This sounds to be a big challenge.[7]

Concerning the second goal, it has been shown, for example, on the bases of a result about exponential separation between certain one-way quantum and classical communication protocols [5], that there are privacy amplification schemes that are secure against classical but not quantum adversaries and a key-expansion scheme in the model of bounded storage cryptography that is secure against classical memory-bounded adversary but not against quantum one [5].

[6] A function f mapping integers into integers is called *negligible* if for any polynomial p and all sufficiently large n it holds $f(n) < \frac{1}{p(n)}$.

[7] Some candidates for such systems are well known: e.g. Diffie-Lamport-Merkle and HFEv signature systems as well as McEliece and (lattice based) NTRU encryption systems, but their security is not well understood yet and their efficiency is not sufficient.

Concerning the third goal, Ajtai-Dwork public-key cryptosystem, based on the computational hardness of the shortest vector problem, that is not known to be solvable by quantum computers, is a candidate.

4. Quantum cryptography

History of quantum cryptography [6] can be seen as starting with Stephen Wiesner's unpublished paper, around 1970, introducing quantum banknotes that would be impossible to counterfeit according to the laws of nature. His ideas inspired Bennett and Brassard's discovery of the quantum key distribution (QKD) protocol BB84 [7]. They also made its toy implementation in 1989—in an experiment with sending and detecting quantum signals (as attenuated laser pulses) over the distance of 32.5 cm.

4.1. *Quantum key distribution*

BB84 was actually the first important discovery showing an extraordinary power of the transmission of quantum states. This protocol provides a so-called *unconditionally secure*[8] method for quantum generation of classical shared, random and secret binary keys.[9] Security of the BB84 protocol depends on the facts that one cannot copy perfectly unknown quantum states and that a measurement of a quantum state does not deform the measured state only in case it is one of the eigenstates of the observable used for the measurement.

The basic idea behind the BB84 protocol is very simple and its unconditional security of BB84 has been proven in many papers under more and more realistic conditions. Commercial products facilitating design of QKD are also already available.

The basic quantum phase of the BB84 protocol goes as follows. To share with Bob n secret random bits, Alice first generates $m > n$ random bits and then sends, subsequently, each of them, say b_i in the i-th step, to Bob using a photon, being randomly either in the state $|b_i\rangle$ or $|\pm_i\rangle$—that is she uses either the standard or the Hadamard basis for the encoding of the bit b_i. After each transmission Bob measures the incoming photon using a randomly chosen basis, either the standard or Hadamard, and records the basis used and also the outcomes of measurements.

After the above process, Bob informs Alice, using a communication through a public authenticated channel, about the sequence of measurements he used, but not about their outcomes. Alice then let him know in which cases he used for measurement the same basis as she did for encoding. The corresponding bits of Alice and Bob create random strings, a pair of so called *raw keys*. They should be same in case there was no eavesdropping and the channel was noiseless. To check for an eavesdropping, Alice and Bob afterwards choose, in a public communication, a set of indices of bits of their raw keys and make public the corresponding bits. In case there is at least a single disagreement in bits in their raw keys and the channel is noiseless, or there are more of them than it is typical for the particular noisy channel, eavesdropping is assumed—otherwise no eavesdropping is expected and the remaining bits are the basis for the rest of the protocol in which, using only classical tools, a care is taken to make sure, using some error-correction techniques, that both parties have the same perfectly random and fully secret key and special *privacy amplification* techniques are used to decouple the resulting key from the eavesdropper.

Unconditional security of BB84 has been proven even for various cases imperfect devices are used [3,8,9]. Three main problems are: imperfection of the sources of photons, noise in channels and imperfection of the detection devices. Because of that a lot of effort has been devoted to the design of practical and sufficiently secure implementations of the BB84 protocol and to the study of potentials of various attacks—actually a whole theory of quantum hacking has emerged, see [8,9].

Since perfect single photon sources are still an experimental challenge, most of the QKD protocols are based on the weak coherent pulses (WCP). However, some of their signals contain more photons prepared in the same polarization state and therefore so-called *Photon Number Splitting* (PNS) attack is possible. As a consequence, BB84 protocols with WCP can provide a key generation rate of

[8]The idea behind unconditional security is simple. By quantum laws, if a quantum state is transmitted an eavesdropper can gain some information about it only using a measurement that will cause disturbance that can be detected by communicating parties. Unconditional security therefore does not mean that an eavesdropper cannot get any information about a state being transmitted; it means only that (s)he cannot get such information without being detected. More exactly, that the amount of information an eavesdropper can get about a generated key goes very fast to zero, with the length of the key.

[9]Generation of secret shared keys is an old and very important problem. Around 1970 secret key generation was seen as the main problem of informatization of society and it was considered to be an unsolvable problem. Diffie and Hellman were the first to provide a computationally secure solution to this problem.

order $\mathcal{O}(\theta^2)$, where θ denotes the transmission efficiency of the quantum channel. To achieve higher security rate over longer distances several other QKD schemes have been developed that are robust against PNS attacks. Very popular is so-called *decoy states* method [10, 8, 9], where the sender randomly varies the mean photon number of the signal states that are forwarded to the receiver. This technique, and some other also, provide a secure key rate of the order $\mathcal{O}(\theta)$. In several QKD schemes the receivers uses two detectors to detect bits 0 and 1. Detection efficiency mismatch is another big issue so serious that it can have fatal effects on practical security. Several attacks have been proposed that make use of detection efficiency mismatch; for example the *time-shift attack*—already demonstrated practically, *faked-state attack* and attacks that make use of the *detectors dead-times*. However, there are ways to deal with such attacks that keep unconditional security, see [11].

A different method of quantum generation of a random and perfectly secure classical binary key was discovered by A. Ekert in 1991 [12], so-called E91 protocol, unconditional security of which is based on the existence of entanglement and security of which can be verified using *Bell inequalities*.[10]

QKD is, on one side, an area in which we have already witnessed great successes with making use of quantum processes to improve solutions of classical tasks. We have QKD protocols that are proven to be unconditionally secure and experimentally verified for distances up to almost 150 km, both in optical fibers and open air [8,9]. Even secure quantum networks, ground-to-satellite and intercontinental secure communication via satellites seems to be feasible using QKD protocols. In addition, it has been demonstrated that the overall goal of QKD, unconditional security, is deeply related to some fundamental and foundational issues of quantum physics (entanglement, testing of Bell-inequalities, detection loopholes, ...).

Unconditional security proofs are not only the highlight of QKD theory, but also, of large importance for its practice [8,9]. Their practical importance is in stating assumptions and formulating pre- and post-processing strategies.

[10]For a modified version of Ekert's protocol, [13] have derived a quantitative bound on Eve's information that depends only on the violation of a Bell inequality. As a consequence they obtained a 'device-independent' bound on security in the sense that it is not required to know neither the dimension of the Hilbert space Alice's and Bob's signals are encoded nor details of measurements performed.

Most of the proofs of unconditional security heavily exploit Hilbert space vision of quantum physics and they use as the underlying assumption that communicating parties know the dimension of the Hilbert spaces their states live in and that the eavesdropper is limited by the laws of quantum mechanics. Surprisingly, the first assumption has turned out crucial, second one not so as discussed later.

An important question is at which error rate (called usually quantum bit error rate (QBER)) is the protocol BB84 secure. Currently the best lower bound is 20% due to [14] and as an upper bound 25% has been determined. To close this gap is an interesting challenge.

4.2. *QKD in non-signaling post-quantum scenarios*

An interesting illustration of the fact that even apparently very simple security problems, as it is the one of the shared secret classical key generation, can lead to deep foundational issues, is to consider whether QKD protocols can be secure even in the presence of an eavesdropper with a *supra-quantum power* and limited only by the non-signaling principle.[11] The fact that no-signaling principle is sufficient to guarantee the security of QKD was first shown in [15]

4.3. *Space-to-ground QKD and global QKD*

There are two main reason why space-to-ground communication, QKD and entanglement distribution is of great interest and experiments are suggested to test how the existing space and ground stations can be used to do that, see [16, 17]. The first one is to test whether we can design a global networks that could lead to QKD much over 1000 km and that way to global QKD and global satellites based and secure quantum communication networks. Second one, to be discussed below, is to create a potential for new tests of the range of quantum mechanics.

[11]Informally this means that the eavesdropper cannot prepare physical systems in a joint state such that a local measurement on one of them may transfer information to another one, even much space separated. In other words, that all correlations she can create have to satisfy the no-signaling condition. More formally, a correlation between two parties, say Alice and Bob, is a conditional probability distribution $P(a, b|x, y)$, where a and b are Alice's and Bob's output data, and x and y are their choices of inputs (say measurements). The no-signaling condition requires that the marginals are independent of the other input, that is $P(a|x, y) = \sum_b P(a, b|x, y) = P(a|x)$.

One idea is that a satellite (say International Space Station) transmits entangled photons to two distant ground stations and by that establishes two different secure keys between the satellite and each of the ground stations. XOR of these keys is then sent publicly to one of the ground stations. This allows to establish an unconditionally secure random key between these two ground stations. For a remarkable proposal along these lines see the project Space-QUEST [17], to be finished in 2014. In the entanglement based satellite-to-ground QKD the idea is that a satellite provides entanglement and distribute it to the communicating parties. Once it would turn out that such ideas are feasible, the door would be open for global secure communication networks.

4.4. *Semi-quantum key distribution*

The fact that on the classical level we cannot have unconditionally secure QKD, but on the quantum level we can, leads naturally to the question how much quantum has to be a key distribution protocol to be robust against attacks. A special version of this question is whether both key generating parties have to be (much) quantum.

Analogical questions have been intensively studied in the area of quantum computation. For example, it has been shown for a special model of classical automata that by adding a single qubit memory one can already asymptotically increase the computational power of automata.

In the paper [18] two protocols for so-called semi-quantum key discrimination have been presented at which Alice is quantum, but Bob is classical in the sense that Bob never works with a superposition of basis states[12] and these protocols are still unconditionally secure. With growing importance of QKD, this line of research is likely to get a momentum.

4.5. *Key distillation as a generalisation of QKD*

It is interesting, important and stimulating to consider QKD also in a more general setting of the so-called key distillation—from the classical or quantum correlations, see [19].

It is also of importance to realize that a QKD protocol can generally be transformed into a key distillation protocol in such a way that security of the latter implies the security of the former [3].

[12] Actually, Bob can do measurement in the classical $\{|0\rangle, |1\rangle\}$ basis, prepare a fresh qubit in one of the states $|0\rangle$ or $|1\rangle$ or reorder the coming qubits (on a channel from Alice to Bob and back).

The general setting for the key distillation is the following one. Communication parties, say Alice and Bob, have access to some correlated pieces of classical or quantum information that might be partially known to the third party, an eavesdropper, say Eve. The goal of Alice and Bob is to distill a (perfectly) random key from these data using only local actions and a public (but authenticated) channel.

It is intuitively clear that this is possible if data Alice and Bob share are sufficiently correlated and Eve's uncertainty about them is sufficiently large. QKD can be seen as a special case of the above distillation problem in the case pre-shared data are generated using a quantum channel.

One of the key issue of the key distillation problem is to determine (at least bounds for) the *key rate*—the amount of key that can be distilled from given date.

An important observation is that the theory of key distillation has parallels with the theory of entanglement distillation that is so much developed. For example, the gap between the *key rate* and the *key cost*—the amount of key needed to simulate pre-shared date using only local actions and public classical communication—can be seen as a classical analogue between *distillable entanglement* (the amount of singlet that can be distilled from a given bipartite quantum state) and *entanglement cost* (the amount of singlets needed to generate the state). As another analogy with entanglement is (still open) question whether there exist *bound information*—classical correlations with the zero key rate, but a positive key cost. Of importance is also the result that there are such entangled states from which one cannot distill any entanglement, but can distill a key, see [20].

4.6. *QKD with finite resources*

Most of the security results for QKD held in the limit. Of large importance for practical QKD, where finite resources are used only, is to determine bounds for secret key rate that can be quite different, as the paper [21] demonstrates, from the asymptotic case.

4.7. *QKD in case eavesdroppers have limited power*

The main goal of QKD is to design key generation protocols that have unconditional security also in the presence of an eavesdropper with power limited only by laws of physics. In some case this is surely much too strong requirement and it is of interest and importance to explore how big security and

how big key rate can be achieved if the power of eavesdropper is somehow limited.

One interesting result along these lines is due to [19]. It deals with the case that eavesdropper has only classical memory. It has been shown that in such a case an arbitrary large separation between the key rate in the unlimited setting and classical memory setting can be exhibited.

4.8. *Perfectly secure transmission of quantum information*

There are two simple methods to achieve perfectly secure transmissions, at least in principle, of quantum information.

If communicating parties share EPR-states, then the quantum teleportation protocol of quantum states can be used to transmit absolutely securely qubits. The catch is again in sharing EPR-states. This has been generalised to achieve transmission of qudits. A more practical protocol, and at the same time theoretically highly inspiring, is the quantum version of the classical one-time pad cryptosystem.[13]

QUANTUM ONE-TIME PAD cryptosystem:	
plaintext:	an n-qubit string: $\|p\rangle = \|p_1\rangle \ldots \|p_n\rangle$
shared key:	two n-bit strings k, k'
cryptotext:	an n-qubit string $\|c\rangle = \|c_1\rangle \ldots \|c_n\rangle$
encoding:	$\|c_i\rangle = \sigma_x^{k_i}\sigma_z^{k'_i}\|p_i\rangle$
decoding:	$\|p_i\rangle = \sigma_z^{k'_i}\sigma_x^{k_i}\|c_i\rangle$
where σ_x and σ_z are Pauli matrices.	

In case of an encryption of a qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ by the quantum one-time pad cryptosystem, what is being transmitted is actually the mixed state

$$\left(\frac{1}{4}, |\phi\rangle\right), \left(\frac{1}{4}, \sigma_x|\phi\rangle\right), \left(\frac{1}{4}, \sigma_z|\phi\rangle\right), \left(\frac{1}{4}, \sigma_x\sigma_z|\phi\rangle\right)$$

whose density matrix is $\frac{1}{2}I_2$ that is identical to the density matrix corresponding to a random bit, represented by the mixed state $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$. Encryption by quantum one-time pad cryptosystem is therefore perfectly secure.

[13] In one-time pad cryptosystem both plaintext (original message) p, cryptotext (encrypted message) c as well as the key k are n-bit strings and the key is always a new random string. Encryption: $c = p \oplus k$ and decryption $p = c \oplus k$ are done by bit-wise xor operation. This is an information perfectly secure cryptosystem which shifts the problem of secure encryption to the problem of generation of random secretly shared key of the same length as the plaintext—this is also the main reason why QKD is so important.

Quantum one-time pad cryptosystem is behind a surprising result that $2n$ bits are sufficient and necessary to hide perfectly n qubits (that can contain unlimitedly large amount of the classical information, hidden in their amplitudes) [22].

4.9. *Quantum cryptographic protocols primitives*

Quantum entanglement is behind the most famous negative results of quantum cryptography. Namely, that there are no unconditionally secure quantum protocols for such cryptographic primitives as *bit commitment* and *oblivious transfer*, see [23]. This has been a very surprising discovery indeed. Another surprising discovery has been that unconditionally secure bit commitment and also oblivious transfer are possible in the so-called *bounded quantum storage model,* where the eavesdropper is expected to have a limited quantum and unlimited classical memory to use, see [24] as discussed later. In addition, even absolutely perfect coin-tossing is not possible in quantum setting. However, it has been shown that there is a quantum protocol for coin-tossing [25], in which neither party can select a desired outcome with probability better than 75%—still much better than what can be achieved classically. An open problem is whether we can have quantum securee protocol for so-called (non-ideal) weak quantum coin-tossing.

The development and study of quantum interactive protocols in general, and quantum zero-knowledge proofs in particular, has been a challenging problem for quantum computation and cryptography. An interesting result concerning zero-knowledge proofs is, see [26], that there are such classical zero-knowledge proofs that are zero-knowledge also against quantum attacks.

4.10. *Cryptographic primitives in special quantum storage models*

It is well known that noise/decoherence is such a big problem for quantum computation that there are still serious doubts whether we can have powerful quantum computers. For example, due to the current and near-future technological limitations it is reasonable to assume that any state placed into quantum memory will be noisy. It is therefore very surprising that noise may have unexpected positive value for quantum cryptography. Indeed, it has been shown in [27], that in the so-called *noisy-quantum storage model* such a basic cryptographic primitive as 1–2 oblivious transfer can be, assuming so-called *individual storage attacks* only, implemented

securely. Namely, that, for the case of depolarizing noise in storage, one can obtaine secure oblivious transfer as long as quantum bit-error rate of the channel does not exceed 11% and the noise on the channel is strictly less than that of quantum storage. This of course implies the existence of robust implementations of other primitives for cryptographic protocols. This result again shows how deeply are related security problems and foundational issues of quantum physics.

Noisy-quantum storage model is not the only model in which one can implement securely such basic cryptographic primitives as 1-2 oblivious transfer—the protocol that one cannot implement in unconditionally secure way when no restrictions on the adversary are made. The second model is *bounded quantum storage model* discussed above. It has been shown that oblivious transfer can be implemented securely as long as a dishonest receiver Bob can store at most $\frac{n}{4} - \mathcal{O}(1)$ qubits coherently, where n is the number of qubits transmitted from Alice to Bob.

4.11. *Quantum multi-party computation secure at the presence of dishonest parties*

Other important cryptographic primitives are protocols for *secure multiparty computations*. The task is to compute, with n parties, $P_1, P_2, \ldots, P_n$, the value of a function $f(x_1, x_2, \ldots, x_n)$ in case that only the party P_i knows x_i and keeps it secret during the computation process. It has been, for example, recently shown, surprisingly, that secret quantum computation is possible for any Boolean function f in such a way that up to $\lceil \frac{n-1}{2} \rceil$ cheaters can be tolerated, see [28]. Both oblivious transfer and bit commitment can be seen as special case of multi-party secure computations.

4.12. *Quantum versus classical cryptography*

There are many natural, but also strange and surprising, ways in which classical and quantum cryptography differ. Let us mention only few of them.

In classical setting we cannot, but in quantum setting we can, detect whether an adversary tried to gain some information, and then to take appropriate actions.

In multiparty classical protocols a party is called honest (but curious) in case it follows perfectly the protocol, but in addition it does some overwork, for example copy for himself available information. A party that does that in quantum protocol can hardly be called honest because copying quantum states causes their disturbance what can, as a consequence, change the result of the protocol, see [2].

Of interest and importance is often to study security of cryptographic protocols for the case the adversary is somehow limited. In the quantum case an important limitation can be the amount of (quantum) storage or types of measurements that can be used. Indeed, in the case of limited quantum memory both bit commitment and oblivious transfer can be implemented securely, see [2]. Moreover, in case there is a limitation on the number of qubits that can be measured at a time, see [29], there is also a secure implementation of the quantum bit commitment.

Very peculiar, and at the same time important and trouble causing, is the fact that if in quantum protocols players postpone measurements, that can have large impacts not only on outputs, but, surprisingly, also on inputs of the protocol. In classical case this has no impacts.

Of importance is also the fact that quantum cryptography involves more than devising quantum protocols for tasks of classical cryptography. Properties of quantum information lead to new cryptographic tasks having no classical counterparts. In addition, relations between classical cryptographic tasks do not apply to their quantum versions. For example, classically so-called (m, n)-string commitment problem is equivalent to bit commitment; but not in the quantum case—unconditionally secure string commitment is possible [30].

Design of a quantum protocol for classical cryptographic task that would precisely replicate a classical protocol, concerning inputs and outputs, contains one subtle problem. Such a protocol would need to verify that its inputs belong to a fixed basis (and so can be seen as classical). This, however, as shown in [31] is not possible in general.

All that demonstrates that the question 'What secrecy means in the quantum world' is non-trivial, intriguing and challenging.

4.13. *Main current challenges of quantum cryptography*

The main challenge is to make QKD systems with better parameters and reliability that would pass "battle testings" and would be interested for market. That requires to keep exploring various new ways to design and implement such systems.

Second main challenge is design of reliable and efficient networks in which communication is protected by QKD systems.

The third main challenge is to extend distances a reliable QKD can work. Losses in all known quantum channels still much limit the distance and key generation rate of QKD. The way to go seems through *quantum repeaters*. Their design is very non-trivial. It requires to build stable quantum memories, efficient quantum error-corrections, as well as interfaces between flying qubits and qubits in memory.

Next challenge is to make ground-to-satellites QKD as well as satellite-to-satellite QKD, and also to link earth-based users by quantum cryptographic processes mediated by satellites. This seems to be feasible and could create a basis for worldwide quantum cryptographic networks.

On the theoretical level, there is also a variety of problems. The first one is of both theoretical and fundamental level. To calculate a real secure key generation rate in noisy channels, or, in other words, quantum bit error rate (QBER). Without that we do not known the actual fundamental limits for QKD. The best lower and upper bounds are known so far (20% and 25%).

5. From quantum cryptography to quantum physics

There is a variety of ways QIPC developments succeeded to put new light on various foundational issues of quantum mechanics. Especially, it helped to put the old questions into brighter relief, to put these questions more clearly and to provide information-theoretic framework in which they can be expressed quantitatively. The overall goal has been nicely formulated by Edwin T. Jaynes:

> Today we are beginning to realize how much of all physical science is really only *information, organized in a particular way*. But we are far from unraveling the knotty question: *To what extent does this information reside in us, and to what extent is it a property of nature?* Our present quantum mechanics formalism is a peculiar mixture describing in part laws of Nature, in part incomplete human information about Nature – all scrambled up together by Bohr into an omelet that nobody has seen how to unscramble. Yet we think the unscrambling is a prerequisite for any further advances in basic physical theory.

A related interesting question is whether also quantum cryptography can help to put new light on foundational issues. More specifically, important questions are whether quantum cryptography can help to derive more natural axioms for quantum mechanics; whether it can help to get more insights into various quantum interpretations and relations among them; whether it can help to get more insight into non-locality issues and to help to explore in more details the power of main quantum resources or even to discover new such resources.

An important, and much related observation in this context, is that of the slogans *Information is physical* and *Physics is informational*, that can and should be extended to understand that also computation, communication, feasibility and secrecy are physical and are therefore important physical concepts.

5.1. *From QKD to new ideas in quantum information theory*

Attempts to find unconditional security proofs for QKD protocols that are as general as possible and also attempts to make long-range, reliable, efficient and fast QKD led also to various new concepts and results in quantum information theory—an area of physics which studies both fundamental and applied issues in quantum mechanics from an information-theoretic viewpoint [2]. Of special importance are generalisations of von Neumann entropy to *smooth min- and max-entropies* and also development of a powerful quantum version of de Finetti's representation theorem [2]. This has in turn led to an important understanding that in order to analyse security of QKD protocols it is generally sufficient to consider only so-called *collective attacks*—where the adversary is restricted to applying the same operation to each particle being transmitted over the communication channel separately.

5.2. *From QKD to new tests of the range of quantum mechanics*

The idea to use open air as communication channel at QKD is as old as the very first experiment. This lead soon to the idea of a ground-space or plane-satellite QKD to renew keys in satellites. Recent progress in entanglement based QKD using open air, especially the one for the distance of 144 km in the Canary Island, opened a new important direction for the fundamental experiments to test the range of quantum mechanics. Namely, can we witness non-local correlations that entanglement should

induce also over macroscopic distances of 1000 and more kilometers?

Quantum laws were established for microscopic objects and distances. There are views that their validity can be restricted to certain mass and length scales and/or they can change under specific gravitational circumstances. The idea to distribute pairs of entangled photons from a satellite to two ground stations and then to make a test for entanglement and non-locality, as elaborated in the project Space-QUEST [17] (that tries to make use of the International Space Station to make proof-of-principles experiments) and also in the project [16] (that tries to test whether Matera Laser Ranging Laboratory facilities can be used for that) and that may open a completely new avenue in testing quantum mechanics. As noted in [16], using large relative velocity of two orbiting satellite, one can even perform experiments on entanglement where, due to special relativity, both observes may claim that they have been performing their measurement prior to the measurement of the other observer. That would give another powerful argument against local realism theory.

5.3. *Deriving quantum mechanics from crypto axioms*

Since special relativity can be deduced from two axioms: the equivalence of inertia reference frames, and the constancy of the speed of light, it is natural to ask would not be possible to deduce also quantum mechanics from some simple axioms that have clear physical meaning? Especially, could we do that using some *information processing based axioms*?

For example, it has been shown, in [32], that observables and state space of a physical theory must be quantum mechanical if the following conditions hold:

- No superluminal information transmission between two systems by measurement on one of them is possible;
- No broadcasting of information contained in an unknown physical state is possible;
- No unconditionally secure bit-commitment is possible.

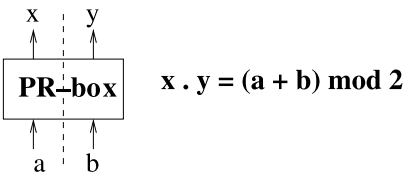
Actually, they have shown that the above constrains force any theory formulated in C^*-algebraic terms to incorporate a non-commuting algebra of observables for individual systems, kinematic independence for the algebras of space-like separated systems and the possibility of entanglement between space-like separated systems.

5.4. *Non-locality issues and quantum cryptography*

Physics was non-local since Newton's time, with exception of the period 1915-1925. Newton has fully realized counter-intuitive consequences of the non-locality his theory implied, but his discovery did not lead to some uproar in physics. Einstein has also realized the non-locality quantum mechanics imply, but this time his, actually the EPR, discovery had big implications on science, in spite of the fact that non-locality quantum mechanics implies does not contradict Einstein' relativity theory. Recently, attempts started to study potential physical theories phenomena of which could provide stronger non-signaling non-locality than the one quantum mechanics allows. It has also turned out to be of interest to study impacts of such potential non-locality on cryptography.

In order to explain such an approach, let us observe that behaviour of a bipartite quantum state under measurement can be described by a conditional probability distribution $P_{xy|ab}$—so called two-party information-theoretic primitive—where a and b denote the chosen bases and x with y are corresponding outputs.

Popescu and Rohrlich [33] introduced so-called *PR-boxes*, as they are called nowadays, that produce stronger than quantum non-local correlations, but still do not allow superluminal communication and therefore do not contradict special relativity.



Let us denote (input) measurements and outcomes by binary values. For the PR-box it holds

$$\text{Prob}[x = y|(a,b) \neq (1,1)] = 1,$$
$$\text{Prob}[x = y|(a,b) = (1,1)] = 0$$

The idea of PR-boxes arises in the following setting: Let us have two parties, A and B, and let one of them, the party X, performs two measurements on a quantum state with outcomes m_0^x and m_1^x with 0 and 1 as potential values. Let us denote a bound on correlations between two such measurements as

$$B = \sum_{x,y\in\{0,1\}} \text{Prob}(m_x^A \oplus m_y^B = x \cdot y).$$

So called Bell/CHCS inequality says that $B \leq 3$ in any classical hidden variable theory. So-called

Cirel'son's bound says that the maximum for B in quantum mechanics is $2\sqrt{2}$.

Popescu and Rohrlich developed, by introducing PR-boxes, a model in which the maximal possible bound, 4, is achievable.

Using PR-boxes one can make bit commitment and 1/2-oblivious transfer unconditionally secure. Having PR-boxes one can simulate any secret multiparty computation and solve any multipartite communication problem by communicating a single bit [34]—what is not possible

Though we know that one cannot realize PR-boxes of interest an importance is the question how well the correlations of PR-boxes can be realized or approximated by devices that follow the laws of physics? In this connection two results are of special interest [35]. The availability of a prior shared entanglement allows to approximate PR-boxes with success probability $\cos^2 \frac{\pi}{8} = 0.854$. Moreover, in no physical world it is possible, without communication, to approximate PR-boxes with probability greater than $\frac{3+\sqrt{6}}{6} \approx 90.8\%$.

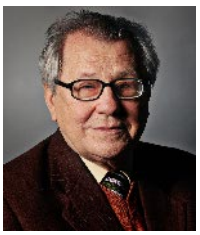
Acknowledgement

Support of the grants GACR 201/07/0603 and MSM0021622419 is to be acknowledged.

Received 16 March 2009.

References

1. J. Gruska, 'A broader view on limitations of information processing and communication by nature', Natural Computing, Springer, V6, 75–112 (2007)
2. S. Wehner, 'Cryptography in a quantum world', PhD thesis, Univ. of Amsterdam, quant-ph/0806.3483
3. R. Renner, 'Security of quantum key distribution', PhD thesis, ETH Zurich, quant-ph/0512258
4. S. Goldwasser and S. Micali, 'Probabilistic encryption', J. Comp. and System Sc., V28, 1073–86 (1984)
5. D. Gavinsky, J. Kempe, I. Kerendis, R. Raz and R. de Wolf, 'Exponential separation for one-way quantum communication complexity, with applications to cryptography', quant-ph/0611209
6. G. Brassard, 'Brief history of quantum cryptography—a personal perspective', quant-ph/0604072
7. C. H. Bennett and G. Brassard 'Quantum cryptography: Public key distribution and coin tossing', Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, 175–179 (1984)
8. H-K. Lo and N. Lütkenhaus, 'Quantum cryptography: from theory to practice', quant-ph/0702202
9. H-K. Lo and Y. Zhao, 'Quantum cryptography', quant-ph/0803.2507
10. W. Y. Hwang, Quantum key distribution with high loss: toward global secure communication', Phys. Rev. Lett, V91, 057901 (2003)
11. C-H. F. Fung, K. Tamaki, B. Qi, H-K. Lo and X. Ma, 'Security proof of quantum key distribution with detection efficiency mismatch', Quantum information and computation, V9, 0131-0165 (2009)
12. A. K. Ekert ' Quantum cryptography based on Bell's theorem', Phys. Rev. Lett., V67, 661-663 91991)
13. A. Acin, N. Brunner, N. Gisin, S. Massar, S. Peronio and V. Scarani 'Device-independent security of quantum cryptography against collective attacks', quant-ph/0702152
14. H. K. Chau 'Practical scheme to share a secret key through a quantum channel with a 27% error rate', Phys.Rev. A, V66, 60302 (2002)
15. J. Barrett, L. Hardy and A. Kent: 'No signaling and quantum key distribution', Phys. Rev. Lett., V 95, 010503 (2005)
16. P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernecehele, V. Luceri, G. Bianco, A. Zeilinger and C. Barbieri 'Experimental verification of the feasibility of a quantum channel between space and earth', New J. Phys., 10;033038 (2008).
17. R. Ursin et al. 'Space-QUEST', quant-ph/0806.0945
18. M. Boyer, R. Gelles, D. Kenigsberg and T. Mor 'Semi-quantum key distribution', quant-ph/0812.4835
19. M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim and R. Renner 'Unifying classical and quantum key distillation', quant-ph/0608199
20. K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim 'Secure key from bound entanglement', quant-ph/0309110
21. V. Scarani and R. Renner 'Security bounds for quantum cryptography with finite resources',quant-ph/0806.0120
22. M. Mosca, A. Tapp and R. de Wolf 'Private quantum channels and the case of randomizing quantum information', quant-ph/0003101
23. J. Gruska, 'Quantum computing', McGraw-Hill, 1999
24. I. Damgård, S. Fehr, L. Salvail and C. Schaffner 'Cryptography in the bounded storage model', Proceedings of 46th IEEE FOCS, 449–458 (2005)
25. A. Ambainis, 'A new protocol and lower bounds for quantum coin flipping', Journal of Computer and System Sciences, V68, 398–416 (2004)
26. J. Watrous, 'Zero-knowledge against quantum attacks', quant-ph/0511020
27. Ch. Schaffner, B. Terhal, S. Wehner 'Robust cryptography in the noisy-quantum-storage model',quant-ph/0807.1333
28. M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, A. Smith 'Secure multiparty quantum computation with (only) a strict honest majority', quant-ph/0801.1544
29. L. Salvail 'Quantum bit commitment from a physical assumption', Proc. of CRYPTO'98, LNCS 1462, 338-353 (1998)
30. A. Kent 'Large N in quantum cryptography', quant-ph/0212043
31. A. Kent 'Promising the impossible: classical certification in a quantum world', quant-ph/0409029
32. R. Clifton, J. Bub, H. Halverson 'Characterizing quantum theory in terms of information theoretic constraints', Foundations of Physics, V33, 1561–1591 (2003)
33. S. Popescu and D. Rohrlich 'Quantum nonlocality as an axiom', Foundations of Physics, V24, 379–385 (1994)
34. W. van Dam, 'Nonlocality & communication complexity', D. Phill. Thesis, Oxford Univ. (2000)
35. G. Brassard, H. Buhrman, N. linden, A. A. Methot, A. Tapp and F. Unger, 'A limit on nonlocality in any world in which communication complexity is not trivial', quant-ph/0508042



Jozef Gruska received PhD from Slovak Academy of Science in 1966. Professor of Faculty of informatics, Masaryk university Brno. Member of Academia Europaea. For 15 years visiting professor at major universities of Europe, North America and Asia. Research interests: parallel automata, descriptional complexity, quantum information processing. The author of two books: Foundation of computing, 1997, International Thomson Computer Press, US,. 730 P., Quantum computing, 1999, McGraw-Hill, UK, 430 p., Founder of 5 series of international conferences. Awards: Bolzano medal of Czech Academy of Sciences, Computer pioneer award of IEEE US.