QUANTUM CHALLENGES OF CRYPTOGRAPHY FOR QUANTUM INFORMATION PROCESSING

Jozef Gruska

Faculty of Informatics, Brno, Czech Republik

March 11, 2008

ABSTRACT I

First goal of the talk is to point out and to demonstrate the key role of security (in a very broad sense) issues in the overall goals of QIPC, both toward new information processing and communication technologies and toward new insights into quantum physics.

- General views on the importance of security.
- Why are security problems so difficult/tricky?
- From classical cryptography to quantum cryptography.
- From quantum cryptography to quantum physics
- From quantum physics to classical cryptography

ABSTRACT II

Second goal of the talk is to discuss in more details results in two areas:

- Generalisation of Quantum One-Time Pad Cryptossystems
- Problems of Anonymity

BASIC POINTS

- Information is physical — physics is informational.
- Computation is physical.
- Communication is physical
- Feasibility is physical
- Security is physical

HISTORY of SECURITY

Development of tools and methods to create “unbreakable security systems” and also of methods and tools to break “unbreakable security systems” have a fascinating history embracing thousands years.

Security tools played an exceptionally important role not only in both world wars, but also much motivated development of the information processing and communication technology.

Computer Collosus, designed to break cryptosystem used for communication between Hitler and his generals, was actually the first very powerful electronic computer.

MODERN CRYPTOGRAPHIC TASKS

To ensure:

- Secrecy of the (transmitted) data (messages) - so that only the intended user finds the content of the (transmitted) data.
- Integrity of the transmitted data - so that one can detected any unauthorized change of the data.
- Signing of the digital data - through digital signatures
- Authentication - of the communicating parties
- Secret sharing and information hiding
- Non-repudiation of activities - a communicating party should not be able to convince other that she did not do what she did.
- Anonymity - of the transmitter or the receiver
- Secrecy at the multiparty computations (at the presence of cheaters)
- Privacy - of the individuals providing information for statistical databases.

FIRST OBSERVATION

Quantum cryptography, as an area of science and technology, should be seen both

as an attempt to develop a new, and more adequate, theory of broadly understood cryptography, and new cryptographic tools and technologies

and also

as a new way to get deeper insights into the information and physical worlds, into their basic concepts, models, laws and limitations.

WHY IS CRYPTOGRAPHY SO MUCH IMPORTANT?

WHY IS CRYPTOGRAPHY SO IMPORTANT? - THREE WARS

- The First World War was a war of chemists - deadly gases.
- the Second World War was a war of physicists - atomic bombs
- Third World War would be a war of cryptographers - information mining and misusing

WHY IS SECURITY SO IMPORTANT - FOUR ERAS

Neolithic era: Progress was made on the basis that men learned how to make use of the potentials provided by the biological world to have **food** available in a sufficient amount and whenever needed.

Industrial era: Progress has been made on the basis that men have learned how to make use of the laws and limitations of the physical world to have **energy** available in a sufficient amount and whenever needed.

Information era: Progress is and will be made on the basis that man learns how to make use of the laws and limitations of the information world to have **information** (processing energy) available in a sufficient amount and whenever needed.

FOURTH ERA - is coming(?)

Security era: Progress is and will be made on the basis that man learns how to make use of the laws and limitations of the physical and information worlds to have **security** available in a sufficient amount and whenever needed.

ARE EFFICIENCY and SECURITY of really great IMPORTANCE and INTEREST?

Two points are crucial:

- Efficiency and security (privacy, anonymity,...) are of the key importance for realization of perhaps the ULTIMATE GOAL (and TOOL) of SCIENCE AND TECHNOLOGY - GRID networks - design of global, information and knowledge accumulating, processing and utilizing, computer networks.
- Paradigms, concepts, models, methods and results concerning efficiency and (computational and communication) complexity one one side, and of the broadly understood cryptography/security on the other side, turned out to be of the key scientific importance for a deep understanding of the physical and information worlds.

GRID NETWORKS - WHAT ARE THEY ABOUT?

- Grids will be very high performance, geographically distributed, heterogeneous, and dynamically changing communication networks of powerful information processing nodes;
- Grids will be enhanced by capabilities to dynamically share information acquiring, storing, processing and transmitting resources (including various sensors, special equipment, ...)
- Grids will allow software, knowledge and physical resources to be shared on scale hitherto unimagined;

WHAT IS THE MAIN MESSAGE CONCERNING SECURITY DESIGN of GRID NETWORKS BROUGHT UP?

So far we have had quite simple and naive views of problems related to security, safety, confidentiality, authentication, anonymity, privacy and so on.

Various ingenious techniques have been developed for handling these problems in a simple environment and as isolated problems.

However, in such a complex and ever changing environment as GRID networks and their variations represent, problems of broadly understood cryptography are getting a new dimension

and

cryptography community starts to understand that it has very little understanding of them and of the way to deal with them.

Concerning security we won many battles, but we are losing the war.

A. Shamir

WHY IS FIGHTING OF INFORMATION MISUSES

IN GRID NETWORKS SO DIFFICULT?

- GRID networks are in principle highly distributed, heterogeneous and evolving,
- GRIDs have no central monitoring and no central control of resources, communications and tasks,
- Networks in general and GRID networks in particular, have many layers and each brings a new type of security problems.

WHY ARE SECURITY PROBLEMS SO DIFFICULT?

Because we need to have a perfect security - less is of not of too much use. Leakage of one bit can be a disaster.

Example RSA cryptosystem

Public key: modulus n, encryption exponent e
Secret key decryption exponent d.

encryption of a plaintext w: $c = w^e$.
decryption of a cryptotext c: $w = c^d$.

Unpleasant fact: If there would be a method to determine, for RSA encryptions, the least significant bit of the plaintext from the corresponding cryptotext, there would exist a method how to determine the whole plaintext from the cryptotext.

THEORETICAL IMPORTANCE of CRYPTOGRAPHY

Fundamental concepts of classical cryptography, and the corresponding laws and limitations, have turned out to be of the key importance for foundation of classical information processing - informatics.

Fundamental concepts of quantum cryptography, and the corresponding laws and limitations, are expected to be of the key importance for foundation of quantum information processing and also informatics and (quantum) physics.

PHYSICS versus INFORMATICS

Basic standpoints

- The main scientific goal of physics is to study concepts, processes, laws and limitations of the physical world.
- The main scientific goal of informatics is to study concepts, processes, laws and limitations of the information precessing world.

Some very basic questions

- What are relations between physical and information worlds? Are they different or two sides of the same world?
- What is the relation between basic concepts, laws and limitations of these two worlds?

CLASSICAL CRYPTOGRAPHY

- Sound approaches:
  - Information theory based approach - enemy should have not enough information to break a cryptosystem.
  - Complexity theory approach - enemy should have not enough computational power to break a cryptosystem.
  - Quantum physics approach - enemy would need to break laws of nature to break a cryptosystem
- Types of perfect secrecy:
  - Absolute (information) secrecy
  - Secrecy computationally indistinguishable from perfect secrecy
  - Unconditional secrecy ensured by physical laws

GOLDWASSER-MICALI DEFINITIONS of CRYPTOSYSTEM SECURITY

They brougt new paradigm into definitions of security in cryptosystems:
Definition – semantic security of encryption A cryptographic system with encryption function e is *semantically secure* if for every feasible algorithm A, there exists a feasible algorithm B so that for every two functions

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

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

$$\text{Pr}[A(e(X_n), h(X_n)) = f(X_n)] < \text{Pr}[B(h(X_n)) = f(X_n)] + \mu(n),$$

where μ is a negligible function.

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

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

MAIN PROBLEMS/AREAS of CRYPTOGRAPHY

- Steganography and watermarking
- Secret-key cryptography
- Secret-key distribution/generation
- Public-key cryptography (RSA an Elliptic curves cryptography, McEllice cryptosystem);
- Digital signatures
- Authentication
- Anonymity
- Privacy

SECURITY in the PRESENCE of ENEMIES

A variety of (external/enemy) attacks on cryptographic systems have been investigated so far. Some of main ones:

- Powerful Eve;
- Man-in-the-middle attacks
- Denial of services
- Attacks on physical systems in use – see attacks on the underlying technology in case of the RSA cryptosystems,

A good theory of (quantum) attacks is needed.

SECURITY in PRESENCE of DISHONEST PARTIES

- In case of multiparty protocols one of the key questions is to ask how many dishonest parties (cheaters) can be tolerated and how to achive that.
- One of main result along this line (quant-ph/0801.1544) says that in the case multiparty quantum computations with n parties up to $\lfloor\frac{n-1}{2}\rfloor$ cheaters can be tolerated by a universally composable protocol.
- In the same paper it has been shown that a verifiable quantum secret sharing is possible in the case of the same number $\lfloor\frac{n-1}{2}\rfloor$ of cheaters.

BEYOND QKD

For a long time quantum genration of classical shared random keys (QKD) has been considered as the key problem of quantum cryptography.

DIMENSION of the KEY GENERATION PROBLEM

1. Around 1970 secret key generation was main problem of informatization of society.
2. Secret-key generation was considered as unsolvable problem.
3. US government distributed several tons of secret keys each day.
4. Main banks had special employees traveling around the world in a briefcase full of secret keys.
5. Secret key generation was enormous logistic problem for armies.
6. Diffie-Hellman brought a solution to this problem.

DIFFIE-HELLMAN SECRET KEY ESTABLISHMENT PROTOCOL

Protocol: If two parties, Alice and Bob, want to create a common secret key, then they first agree, somehow, on large prime p and a primitive root $q \ (\mathrm{mod} p)$ and they perform through public channel the following activities.

- Alice chooses, randomly, a large $1 \leq x < p - 1$ and computes $X = q^x \bmod p$.
- Bob also chooses, randomly, a large $1 \leq y < p - 1$ and computes $Y = q^y \bmod p$.
- Alice and Bob exchange X and Y, through a public channel, but keep x, y secret.

- Alice computes $Y^x \bmod p$ and Bob computes $X^y \bmod p$ and then each of them knows the key $K = q^{xy} \bmod p$

SECURE ENCRYPTION WITHOUT KEYS

Let Alice uses cryptosystem with encryption mapping e_A and decryption mapping d_A and let Bob uses cryptosystem with mappings e_b and D_B and let these two cryptosystems are commutative.
Secure sending of a message m.

1. Alice sends $e_A(m)$ to Bob;
2. Bob sends $e_B(e_A(m))$ to Alice
3. Alice computes $d_A(e_B(e_A(m))) = e_B(m)$ and sends $e_B(m)$ to Bob;
4. Bob gets m

SECURE QUANTUM ENCRYPTIONS WITHOUT KEYS

QUANTUM SECURE DIRECT COMMUNICATION - QSDC

- It allows that the sender transmits directly the secret to the receiver in a deterministic and secure matter.
- A carefully designed QSDC can also attain unconditional security in theory.
- At the beginning the communications in QSDC protocols were along one direction, from Alice to Bo b.
- Subsequently, protocols of bidirectional QSDC, or so-called quantum dialogue, were proposed, whe re secret messages can flow in both directions.

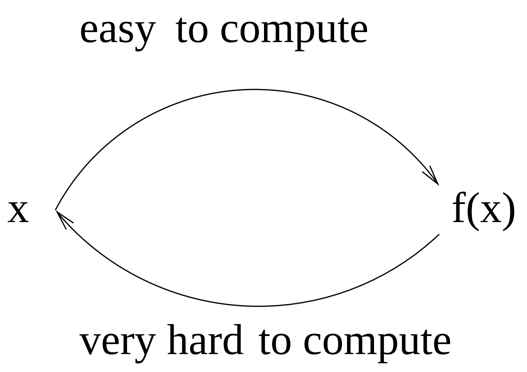
IMPORTANCE of CLASS. CRYPT. CONCEPTS for FOUNDATIONS of INFORMATIC

Key concepts of classical public-key cryptography have turned out to be key concepts of foundations of informatics:

- one-way functions;
- trapdoor one-way functions;
- hard-core predicates;
- interactive proofs
- zero-knowledge proofs
- holographic proofs;
- cryptographic-perfect pseudo-random generators;
- universal sets of hashing functions

ONE-WAY FUNCTIONS

One-way functions are functions that are **easy** to compute, but **hard** to invert. (It is easy to specify what *easy* means, but it is very hard to specify what *hard* means.



DEFINITION and SOME IMPORTANT OUTCOMES

- Definition: A function $f : \{0,1\}* \rightarrow \{0,1\}^*$ is one-way if

  (a) f is easy to compute;

  (b) there are $c, \varepsilon > 0$ such that $|x|^\varepsilon \leq |f(x)| \leq |x|^c$ and (c) For every randomized polynomial time algorithm $\mathcal{A}$ and any $c > 0$ there exists an N such that for any $n > N$

$$Pr(\mathcal{A}(f(x)) \in f^{-1}(f(x)) \leq \frac{1}{n^c}.$$

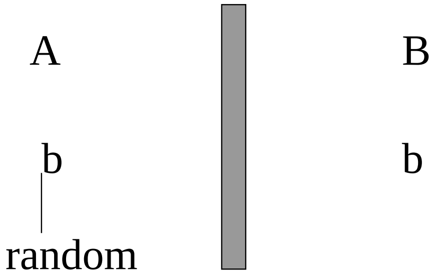
- Some of main results:
  - One-way functions exists if and only if $\mathbf{P}$ = $\mathbf{UP}$.
  - There is a generic/complete one-way function - a function that is one-way iff one-way functions exist.

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, . . .) - even if a certain number of parties are malicious (may cheat).
- Oblivious transfer, 1-out-of-2 oblivious transfer, bit commitment and (long-distance) coin-tossing are main primitives of cryptographic protocols.
- Using oblivious transfer one can implement securely bit commitment and using bit commitment one can implement coin-tossing protocol.
- Using oblivious transfer one can implement securely any multiparty computation at which each party keep secret its inputs.

PRIMITIVES of CRYPTOGRAPHIC PROTOCOLS

Coin−flipping

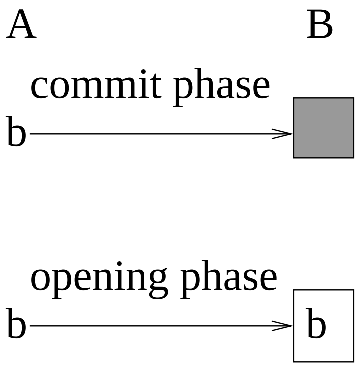


A B

b b

random

Bit commitment



A B

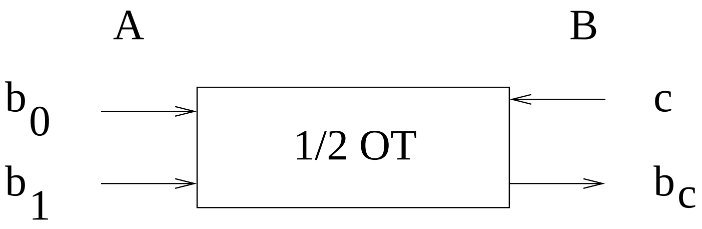
commit phase

b

opening phase

b b

1/2 oblivious transfer



A B

b_0 c

1/2 OT

b_1 b_c

SECURITY of CRYPTOGRAPHIC PROTOCOLS - I. PROBLEMS

In the case of cryptographic protocols new circumstances come into considerations when security is considered.

- Cryptographic protocols are used in a complex environment like internet. The problem is that such protocols are usually designed as stand-alone, not to be run concurrently with other protocols.
- The starting point at the design of cryptographic protocols is usually an informal description of a cryptographic task. On this basis a protocol that is to implement the task is designed. The question then is how to prove that protocol really meets the task and it is secure (at each use).
- The ways how security of a protocol is defined usually keep changing for different tasks.

WHAT IS NEEDED?

We need definition of security that would be sufficiently general, uniform and robust. A definition that would allow:

- to prove security quite easy;
- to compose protocols;
- to handle complex network environment;
- to analyse classes of protocols;
- to develop formal and automatic tools to prove security;
- to deal with classical and quantum protocol in a sufficiently uniform way;
- to understand better cryptography and the also the laws and limitations of information processing world.

COMPOSABILITY

- Cryptographic protocols (especially such primitive ones as BC (bit commitment) and OT (Oblivious transfer) are almost never executed on their own. They are usually used as building blocks of more complex applications.
- It is already known that composition of secure protocols does not have to be secure.
- A very important and difficult problem in protocol design is therefore their composability.
- Two main types of composability are sequential composability and universal composability
- Sequential composability means that protocols can be composed in an arbitrary way, as long as in any point of time exactly one protocol is running - all other protocols have to wait until that protocol stops.
- 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 **simuator** 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.
- To make the protocol sequentially composable, we have to allow the adversary to receive some **auxiliary input** from the environment, which could contain, for example, information from previous runs of the protocol,...

BASIC PRIMITIVES of QUANTUM CRYPTOGRAPHY

- 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;
- Identification and authentication protocols
- Quantum protocols to share and hide classical and quantum information
- Anonymity protocols (Bouda, Šprojcar 2006).

QUANTUM ONE-TIME PAD CRYPTOSYSTEM

CLASSICAL ONE-TIME PAD cryptosystem

plaintext: an n-bit string p
shared key: an n-bit string k
cryptotext: an n-bit string c
encoding: $c = p \oplus k$
decoding: $p = c \oplus k$

QUANTUM ONE-TIME PAD cryptosystem:

plaintext: an n-qubit string $|p\rangle = |p_1\rangle \dots |p_n\rangle$
shared key: two n-bit strings k, k'
cryptotext: an n-qubit string $|c\rangle = |c_1\rangle \dots |c_n\rangle$
encoding: $|c_i\rangle = \sigma_x^{k_i} \sigma_z^{k'_i} |p_i\rangle$
decoding: $|p_i\rangle = \sigma_z^{k'_i} \sigma_x^{k_i} |c_i\rangle$

UNCONDITIONAL SECURITY of QUANTUM ONE-TIME PAD

In the case of encryption of a qubit

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

by QUANTUM ONE-TIME PAD cryptosystem what is being transmitted is the mixed state

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

whose density matrix is

$$\frac{1}{2}I_2.$$

This density matrix is identical to the density matrix corresponding to that of a random bit, that is to the mixed state

$$(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$$

SHANNON's THEOREMS

Shannon classical encryption theorem says that n bits are necessary and sufficient to encrypt securely n bits.

Quantum version of Shannon encryption theorem says that $2n$ classical bits are necessary and sufficient to encrypt securely n qubits.

FROM QUANTUM ONE-TIME PAD TO QUANTUM PRIVATE CHANNELS

A natural way to generalize one-time pad cryptosystem is that of **quantum private channel** – a synonym for a perfectly secure encryption by perfect ran domizat ion for sending messages through noiseless one-way quantum channel.

Basic scenario for a **quantum private channel (QPC)** is that:

- There are m possible keys - unitary matrices U_i, $i = 1, \ldots, m$, over n-qubits, and unitary U_i is chosen with probability p_i;
- Sending, by Alice, of a state $|\phi\rangle$, from a set $\mathcal{S}$ of states, amounts to multiplying at first $|\phi\rangle$ with a randomly chosen U_i and then sending the resulting state;
- Decoding is done by selecting, using shared randomness, and then applying the inverse unitary $U_i^\dagger$;

- Such a protocol is perfectly secure if for all states $|\phi\rangle$ it holds

$$\sum_{i=1}^{m} p_i U_i |\phi\rangle\langle\phi| U_i^\dagger = \frac{1}{2^n}\mathbf{I}_{2^n}. \tag{1}$$

- If this is the case, we say that the probability distribution $\{(p_i, U_i)\}_i$ specifies a private quantum channel.

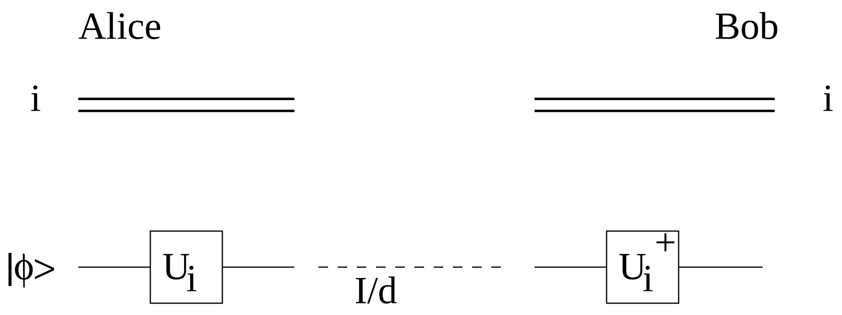


Figure 1: A quantum private channel based on randomization

Indeed, if (1) is satisfied, then an eavesdropper cannot learn anything about the state being sent.

A MORE GENERAL VIEW OF QUANTUM PRIVATE CHANNEL

General case is that the sender/Alice first attaches an ancilla ρ_a to the state $|\phi\rangle\langle\phi|$ to be sent and then randomizes the composed state.

In addition, one should consider also the cases that only states from a special set of states are being transmitted. This leads to the following definition (Mosca et al. 2000):

Definition 0.1 *Let $\mathcal{S}$ be a set of n-qubit states, $\mathcal{E} = \{\sqrt{p_i}U_i \,|\, 1 \leq i \leq k\}$ be a superoperator with U_i being unitaries on an $m \geq n$ qubit register, $\sum_{i=1}^{k} p_i = 1$, and ρ_a be an $(m-n)$-qubit density matrix. $[\mathcal{S}, \mathcal{E}, \rho_a, \rho_0]$ specifies a* private quantum channel *if and only if for all $|\phi\rangle \in \mathcal{S}$ it holds*

$$\mathcal{E}(|\phi\rangle\langle\phi| \otimes \rho_a) = \sum_{i=1}^{k} p_i U_i(|\phi\rangle\langle\phi_i| \otimes \rho_a)U_i^{\dagger} = \rho_0.$$

FROM QUANTUM PRIVATE CHANNEL to (APPROXIMATE) RANDOMIZATION

The concept of QPC is closely related to that of randomization (or forgetting) of quantum information/states and the achievable.

The lower bound for the number of bits needed for QPC is actually the amount of entropy, or the thermodynamical cost, of randomization/forgetting.

Basic definition and result concerning approximate randomization have the following form.

Definition 0.2 *A superoperator $\mathcal{R}$ on $\mathcal{H}_d$ is an ε-randomizing map if, for all pure states $|\phi\rangle$,*

$$||\mathcal{R}(\phi) - \frac{\mathbf{I}_d}{d}||_\infty \leq \frac{\varepsilon}{d}.$$

DETAILS and FURTHER DEVELOPMENTS

- Hayden et al (2004) studied the case that the distance between the cryptotext and maximally mixed state be smaller than some security parameter ε.
- They proved existence of an encryption scheme such that the key length is $n + \log n + 2\log(1/\varepsilon)$.
- Later Ambainis and Smith (2004) showed that one can do encryption using only $n + 2\log(1/n)$
- Desrosiers (2007) developed encryption scheme that uses $n - t + \log(1/n)$ bits of key to encypt n qubits, where t is min-entropy of the adversary on the message space - in some cases therefore number of bits of the key can be smaler than n.

ENTROPY of the KEY

- Problem Given a set P of plaintext states. What is the entropy of the key necessary and sufficient to encrypt plaintext states from P.
- A sinle bit of key is sufficient when the set P is two dimensional.
- The necessary and sufficient entropy of the key in cas P is three dimensional varies continuously between 1 and 2 bits (Bouda, ziman, 2007).

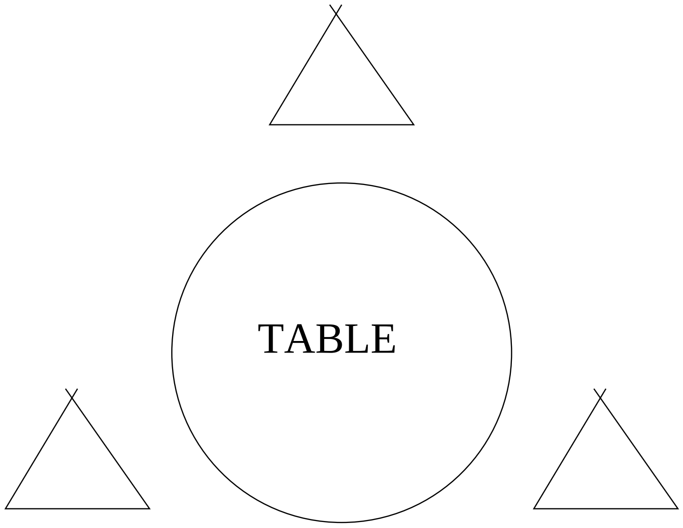
ANONYMITY

- There are many types of anonymity; sender/receiver anonymity, relationship anonymity,...
- In a narrow sense ”anonymity means hiding identities of parties”.
- In a broader sense ”anonymity is the state of being not identifiable within a set of subjects (within so-caqlled anonymity set).
- Anonymity is widely used in practice nowadays.
- Two main applications: e-voting and e-commerce (manipulation of e-money).
- Some anonymity applications, especially last two, are highly complicated and anonymity is an essential part of them.
- To develop good models and theory of anonymity and of security of anonymity protocols is a big challenge (of current classical and also quantum cryptography).

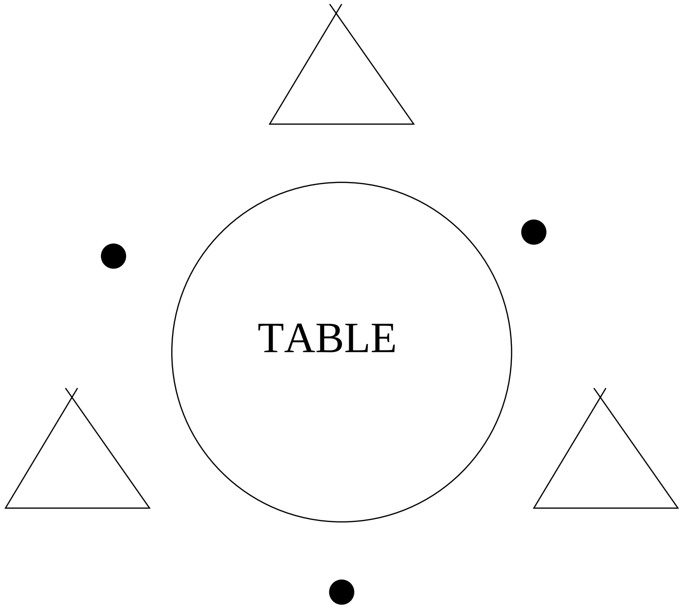
ANONYMITY - THE DINING CRYPTOGRAPHERS PROBLEM

- **Three cryptographers have dinner at a round table of a 5-star restaurant.**
- **Their waiter tells them that an arrangement was made that their bill will be paid anonymously - either by one of them, or by NSA.**
- **They respect each others right to make an anonymous payment, but they wonder if NSA has payed the dinner.**
- **How should they proceed to learn whether one of them paid the bill without learning which one - for other two?**

*****



TABLE



TABLE

DINNING CRYPTOGRAPHERS - SOLUTION

- Protocol
  - **Each cryptographer flips a perfect coin between him and the cryptographer on his right, so that only two of them can see the outcome.**
  - **Each cryptographer who did not pay dinner states, aloud, whether the two coins he sees - the one he flipped and the one his right-hand neighbour flipped - fell on the same side or on different sides.**
  - **The cryptographer who paid the dinner states, again aloud, the opposite what he sees.**
- Correctness
  - An odd number of differences uttered at the table implies that a cryptographer paid the dinner.
  - An even number of differences uttered at the table implies that NSA paid the dinner.
  - In a case a cryptographer paid the dinner the other two cryptographers would have no idea who paid the dinner.

ANONYMITY SCENARIO

- There is a set S of parties that includes a subset A of potential anonymous sender/receiver an A contains a set An of anonymous senders/receivers.
- There is a subset $F \subset S$ of **friends** of An that includes An.
- There is a subset $O \subset S - F$ of observers that try to determine an $P \in An$.
- The goal of observers from O is to find at least one $P \in An$.
- The task is design such a protocol that parties in O are not able to determine any element in An by a probability larger than guessing provides.

ANONYMOUS CHANNELS

An anonymous channel is a cryptographic protocol modeling (complex) communication patterns with several anonymous actions performed on several messages by several parties.

Observe that the above definition of Anonymous channel is built on top of the definitionof anonymity.

Formally: An anonymous channel is $ACh = (P, M, a, A, F)$, where

- P is a set of parties;
- M is a set of messages;
- $a : P \times M \rightarrow \{\text{send}, \text{receive}\}$ - description of the communication pattern in the channel;
- $A : P \times M \rightarrow 2^P$ - anonymous set of a particular party for a particular message;
- $F : P \times M \rightarrow 2P$ - a set of friends of a party X when performing an action on a message m;

satisfying certain (natural) properties -Šprojcar (20080),

SECURITY PROPERTY

Correctness . Let $C \subseteq P$ be a set of **corrupted parties**.

$$\forall x \in P - C, \forall m \in M \text{ if } a(x,m) \text{ is defined}$$

then $a(x,m)$ is peformed by the protocol – in other words, physical actions of the (real) protocol implement all logical actions specified in the definition.

Anonymity • If $F(x,m) \cap C \neq \emptyset$ then anonymity of x performing an action on m is trivially broken.

ANONYMOUS SENDING of QUANTUM INFORMATION

BASIC IDEA: If an (anonymous) sender S achieves an anonymous sharing of EPR pairs with the sender R, then anonymous transmission of quantum information from S to R can be achieved using teleportation.

BASIC TRICK: If $n+1$ parties share the state

$$\frac{1}{\sqrt{2}}(|0^{(n+1)}\rangle + |1^{(n+1)}\rangle)$$

and $n-1$ of them measure their particles in the dual basis, then the remaining two parties share either the EPR state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{or} \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

J. Bouda, J. Šprojcar, quantum archive

QUANTUM MTAS - SIMPLIFIED VERSION - Bouda, Šprojcar (2006)

- All parties agree publicly on a set of quantum purity testing codes $\{Q_k\}_{k=1}^{?}$ that map m_1 qubits to m;
- An anonymous EPR-pair distribution is repeated m_1 times;
- S chooses a purity testing code Q_{k_0} and sends k_0 to R using classical MTAS;
- R measures syndrome of the code Q_{k_0} and sends the result to all parties;
- S measures the syndrome of the code Q_{k_0} and compares it with the syndrome received from R. If they are the same, with high probability s and R share m EPR-pairs.
- S teleports the message **mess** using shared EPR-pairs and send s the outcomes of Bell measurement using classical MTAS.

ANONYMOUS EPR-PAIR DISTRIBUTION - ONE ROUND

(Also a way to check for cheating.)

1. S decides whether this is to be an actual or a trap round and announces decision to R using classical MTAS;
2. If a trap round: R sends to each party P_i randomly $|0'\rangle$ or $|1'\rangle$ and remembers it;
3. if an actual round: R prepares state $\frac{1}{\sqrt{2}}(|0^{(n+1)}\rangle + |1^{(n+1)}\rangle$ and sends one qubit to each of n parties;
4. Each party P_i except S measures its qubit in dual basis and records the outcome x_i;
5. If a trap round: S also performs the measurement as others; otherwise s does nothing.
6. All parties anonymously agree on their ordering and each sends its x_i to S using classical MTAR;
7. If a trap round: S sends all (i, x_i) using classical MTAS to R; if any of x_i differs from what R sent, R concludes that P_i is cheating - announces it and protocol restarts, Cheating participants are excluded from anew execution of the protocol;
8. If an actual round: S repairs the state S shares with R to get an EPR-pair - by applying σ_z if $\oplus_i x_i = 1$.

FROM (QUANTUM) CRYPTOGRAPHY TO (QUANTUM) PHYSICS

SOME of FUNDAMENTAL QUESTIONS

CRYPTOGRAPHY COULD HELP TO ANSWER

- **Is our universe a polynomial or an exponential place?**
- **How real and useful is (quantum) randomness quantum measurement produces?**
- **How real and useful is quantum entanglement and what are the laws and limitations of quantum entanglement?**
- **What kind of non-locality we can have that does not contradict the relativity theory?**
- **How to distinguish between various interpretations of quantum mechanics?**

CAN QUANTUM CRYPTOGRAPHY HELP TO ANSWER QUESTION

WHY QUANTUM MECHANICS?

Can we have for QM axioms whose physical, or better yet information-theoretic or information-processing, meaning is clear - so we will have a particularly nice answer to the question ”Why quantum mechanics”.

It is hoped/believed that QIPCC science will be a useful new source of axioms, with natural interpretations involving the possibility or impossibility of various information processing processes.

Quantum computational complexity has already been used to show why various modifications (or *fantasy versions*) of quantum mechanics are much too powerful and this way we can gain an insight why quantum mechanics is as it is.

CAN QUANTUM MECHANICS BE DERIVED FROM

SECURITY AXIOMS?

Open problem. Can we built quantum physics from the following two axioms

- Unconditionally secure quantum key distribution is possible.
- Unconditionally secure bit commitment is not possible.

and, perhaps, of few other axioms?

ARE THERE NEEDS FOR BETTER AXIOMS OF QM?

- Basic question: Since special relativity can be deduced from two axioms: the equivalence of inertia reference frames, and the constancy of the speed of light, could not be possible to deduce also quantum mechanics from some simple axioms that have clear physical meaning?
- Could we do that using some information processing based axioms?
- Fuchs and Brassard suggested to consider as axioms (a) the existence of unconditionally secure cryptographic key generation and (b) together with impossibility of secure bit commitment.
- One such attempt was done by Clifton, Bub and Halvorson with three axioms: No signaling, no broadcasting and no bit commitment.
- Could derivation of such axioms be a common task for (quantum) physics and (quantum) informatics?

CBH THEOREM

Clifton, Bub and Halverson (2002) have shown that observable 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;
- no broadcasting of information contained in an unknown physical state;
- No unconditionally secure bit-commitment

Actually they showed 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.

SECURITY versus INTERPRETATIONS of QUANTUM THEORY

- It is well-known that statistical predictions of quantum theory do not depend on its interpretat ion.
- In particular, an experiment cannot distinguish between Copenhagen interpretation (involving no hidden variables) and the de Broglie-Bohm interpretation based on nonlocal hidden variables.
- Quantum cryptographic protocols for classical key generation, such as BB84 and E91, are secure a nd mutually equivalent as long as one works within the framework of Copenhagen interpretation.
- However, they are inequivalent and insecure if one considers attacks allowed by the de Broglie-B ohm interpretation.
- Ekert-type protocols can be modified in a way that makes them secure even if the de Broglie-Bohm nonlocal hidden variables exist. This does not seem to be the case for Bennett-Brassard protocols.

Pawlowski, Czachor - quant=ph/0412058

FUNDAMENTAL PROBLEM of QUANTUM CRYPTOGRAPHY

Are all statements about security of quantum cryptographic protocols based on our belief in an interpretation of quantum mechanics?

HOW CAN QUANTUM PHYSICS HELP TO CLASSICAL CRYPTOGRAPHY

- It could perhaps help to handle security problems in communication (network) channels in a more unified way - classical network channels consists of several levels and they have their own security problems.

CHANGING WORLD

Views on the role of physics in the understanding of the physical world keep developing.

- **Nothing exists except atoms and empty space; everything else is opinion.** ***Democritus of Abdera (ca. 400 BC)*****.**
- **In Science there is only Physics: all the rest is stamps collecting.** ***Ernest Rutherford (1912)***
- **Physics is like sex; it produces sometimes practical results, but this is not reason why we do it. Feynman (19??)**
- **Physics is not the only science to get deep understanding of physical world. Informatics can and should help.**