CENTRAL EUROPEAN QUANTUM INFORMATION PROCESSING WORKSHOP

CEQIP 2012

7-10, June, 2012
Smolenice Castle, Slovakia
http://www.ceqip.eu/2012/

CEQIP'12 (Central European Quantum Information Procesing workshop) is focused on current challenges and paradigms of quantum information processing. Although the workshop is open for any topic of quantum information theory, this year we plan to focus more on quantum randomness, novel schemes for quantum communication, quantum entanglement theory and novel algorithms for simulations of quantum systems.

PROGRAM COMMITTEE:
Andris Ambainis, Časlav Brukner, Jan Bouda, Jens Eisert, Beatrix Hiesmayr, Daniel Nagaj, Martin Plenio, Mario Ziman

ORGANIZERS:
Jan Bouda (Czech Republic), bouda@fi.muni.cz
Martina Zemanová (Slovakia), martina.zemanova@savba.sk
Mário Ziman (Slovakia), mario.ziman@savba.sk

The workshop is organized by Quantum Laboratory, Faculty of Informatics, Masaryk University (Brno) and Research Center for Quantum Information, Institute of Physics, Slovak Academy of Sciences (Bratislava).

INVITED TALKS

Dagmar Bruss (Dusserdorf, Germany)
Properties of quantum correlations
Composite quantum systems that cannot be described by joint classical probability distributions exhibit quantum correlations. In this talk some of their properties will be illustrated: are quantum correlations monogamous? How do they behave under the action of local channels? These investigations may help to understand the role of such correlations in information processing.
FRIDAY, 15:30

Teiko Heinosaari (Turku, Finland)
Invitation to quantum measurements
Considering quantum theory as a framework for calculating measurement outcome probabilities, it has aspects which make it both a generalization and a restriction of the usual probability theory. It is a generalization in the sense that observables are described by positive operator valued measures. These are more general than probability measures, in much same way as matrices are more general than numbers. However, quantum theory imposes inherent restrictions on the probability distributions that we can find in quantum measurements. In this sense, it can also seen as a restriction of the usual probability theory. This talk is a short tutorial on quantum measurements. Topics will include observables, instruments, incompatibility and disturbance. Both aspects, generalization and restriction of the usual probability theory, will be discussed through examples.
SATURDAY, 10:30

Mark Hillery (New York, United States)
Quantum Machines - a Strange History
We review the history of quantum machines, starting with the discovery of the no-cloning theorem, which was motivated by a super-luminal communication scheme put forward by a group of unorthodox physicists. We discuss the history of this group and some of their unusual preoccupations. We then go on to review some results about quantum cloning and programmable quantum machines. This is meant to be a fun talk, and it is suggested that the audience bring a glass of wine with them.
SATURDAY, 18:30

Pawel Horodecki (Gdansk, Poland)
Form entanglement-based superadditivity of information transfer to percolation phenomena
Superadditivity results on classical information via quantum information transfer will be reviewed inluding recent results showing the role of multipartite entanglement. The new type of directed percolation phenomena basing directly on superadditivity of capacities in quantum network will be presented.
THURSDAY, 17:50

Debbie Leung (Waterloo, Canada)
Nonlocality without entanglement revisited
Bennett, DiVincenzo, Fuchs, Mor, Rains, Shor, Smolin, and Wootters found a bipartite product basis that cannot be distinguished by LOCC with arbitrary precision. In this talk, a simplified proof and extensions to other product basis will be presented. Thoughts on LOCC and SEP will be discussed if time permits. Joint work with Andrew Childs, Laura Mancinska, and Maris Ozols.
FRIDAY, 14:00

Joe Renes (Zurich, Switzerland)
Quantum Polar Coding
Polar coding, introduced 2008 by Arikan, is the first (very) efficiently encodable and decodable coding scheme whose information transmission rate provably achieves the Shannon bound for classical discrete memoryless channels in the asymptotic limit of large block sizes. In this talk I describe how polar codes can be used for the transmission of quantum information. For qubit Pauli channels and qubit erasure channels, a quantum coding scheme can be constructed from classical polar codes which, using some pre-shared entanglement, asymptotically achieves a net transmission rate equal to the coherent information using efficient encoding and decoding operations and code construction. When the noise rate is sufficiently low, the rate of preshared entanglement required is in fact provably zero. An essentially identical construction works to achieve the coherent information for arbitrary channels, but as yet it is not known if one can construct an efficient decoder.
FRIDAY, 9:00

Frank Verstraete (Wien, Austria)
Quantum Hypothesis testing
THURSDAY, 16:20

Andreas Winter (Singapore / Bristol, United Kingdom)
Towards a strong converse for the quantum capacity of degradable channels
The (weak) capacity of a quantum channel is defined as the largest rate of qubits in an asymptotically error-free code. By contrapositive, for rates above the quantum capacity, the error cannot go to zero for asymptotically many uses of the channel. Motivated by classical Shannon theory, where such statements are true, we ask whether the "strong converse" holds: i.e., for rates above the quantum capacity, does the error actually tend to 1? The strong converse would not only have applications in the cryptographic use of noisy channels, but would foremost be of conceptual value, as it says that there is no rate-error trade-off in noisy channel coding. We show a step towards a strong converse for the quantum capacity. To be precise, we can prove that if there is a rate-error trade-off, then it is very weak: Indeed, our "semi-strong converse" states that for the class of degradable channels, coding of rate above the quantum capacity necessarily has a certain universal constant error, asymptotically [Reporting joint work in preparation with Ciara Morgan.]
FRIDAY, 10:30

LIST OF POSTERS

1. Tomer Jack Barnea: The hidden influence polytope in the tripartite case
2. Jan Bouda, Matej Pivoluska, Martin Plesch, Colin Wilmott: Quantum encryption with weak randomness using multi-qubit ciphertexts
3. Jordi Tura Brugués, Remigiusz Augusiak, Philipp Hyllus, Marek Kus, Jan Samsonowicz and Maciej Lewenstein: Four-qubit PPT entangled symmetric states
4. David Edward Bruschi, Andrzej Dragan, Eduardo Martin-Martinez and Jason Doukas: Localised projective measurement of a relativistic quantum field in non-inertial frames
5. Michał Cholewa, Piotr Gawron and Przemysław Głomb: Transition Operation Matrices based Quantum Hidden Markov Models
6. Michal Daniška and Andrej Gendiar: Suppression of Finite Size Effects by Sine Deformation
7. Paul Erker, Marcus Huber, Hans Schimpf, Andreas Gabriel and Beatrix Hiesmayr: Detecting genuine multipartite entanglement in Dicke states
8. Julio de Vicente, Tatjana Carle, Clemens Streitberger and Barbara Kraus: Complete set of operational measures for the characterization of three-qubit entanglement
9. Andrej Gendiar: Phase Transitions on Non-Euclidean Hyperbolic Geometries
10. Erkka Haapasalo: Extreme covariant quantum observables in the case of an Abelian symmetry group and a transitive value space
11. Pankaj Joshi, A Grudka, K Horodecki, M Horodecki, P Horodecki and R Horodecki: No-broadcasting of non-signalling boxes via operations which transform local boxes into local ones
12. Michael Nölle, Martin Suda and Ian Glendinning: Conjugate Variables as a resource for information processing
13. Nikola Paunkovic, Jan Bouda, Paulo Mateus and Daowen Qiu: Quantum commitments based on complementarity
14. Łukasz Pawela and Jan Sładkowski: Quantum Prisoner's Dilemma game on hypergraph networks
15. Zbigniew Puchała, Wojciech Roga and Karol Życzkowski: Entropic uncertainty relation for quantum operations
16. Peter Rapčan, Mário Ziman, Jochen Rau and Vladimír Bužek: Estimation of decoherence channels
17. Daniel Reitzner, Teiko Heinosaari and Takayuki Miyadera: Compatibility of measurement devices
18. Tomáš Rybár, Mário Ziman and Vladimír Bužek: Estimating 2 qubit interaction in memory channel setting
19. Przemysław Sadowski: Generating quantum circuits preparing maximally entangled states
20. Stefan Schauer and Martin Suda: Security of Entanglement Swapping QKD Protocols against Collective Attacks
21. Łukasz Skowronek: Generation of mapping cones from small sets
22. Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos and Beatrix Hiesmayr: Entanglement detection via mutually unbiased bases
23. Anna Szymusiak: Entropy of group covariant quantum measurement
24. Jan Vlach, Michael Krbek and Tomáš Tyc: Reachable states of subsystems of N modes of electromagnetic field
25. Colin Wilmott: Deriving a basis for the set of bounded operators on a finite-dimensional Hilbert space
26. Abuzer Yakaryilmaz: Turing-equivalent automata using a fixed-size quantum memory
27. Mário Ziman, Tomáš Rybár, Sergey N. Filippov, Vladimír Bužek: Simulation of indivisible qubit channels in collision models

CONFERENCE PROGRAM

THURSDAY, 7.6.2012
14:30 Registration
15:40 Opening coffee break
16:20 **Frank Verstraete:** Quantum Hypothesis testing
17:05 **Xiaotong Ni:** Commuting quantum circuits: efficient classical simulations vs hardness results
17:30 Break & Refreshment
17:50 **Paweł Horodecki**: tba
18:35 **Daniel Nagaj:** Quantum Speedup by Quantum Annealing
19:00 WELCOME DINNER

FRIDAY, 8.6.2012
08:00 Breakfast
09:00 Morning session
09:00 **Joe Renes:** Quantum Polar Coding
09:45 **Gabriele De Chiara:** Entanglement spectrum and order parameters in strongly correlated systems
10:10 Break & Refreshment
10:30 **Andreas Winter:** Towards a strong converse for the quantum capacity of degradable channels
11:15 **Josh Cadney:** Infinitely many constrained inequalities for the von Neumann entropy
11:40 **Nikolajs Nahimovs**: Better algorithms for search by quantum walk on two-dimensional grid
12:05 End of session
12:15 Lunch
14:00 Afternoon session
14:00 **Debbie Leung:** Nonlocality without entanglement revisited
14:45 **Marcus Huber:** Exploring multipartite entanglement
15:10 Coffee & Refreshment
15:30 **Dagmar Bruss:** Properties of quantum correlations
16:15 **Michal Studzinski:** Distillation of entanglement by projection on permutationally invariant subspaces
16:40 **POSTER SESSION**
18:45 SOCIAL DINNER
19:30 CIPHER GAME
00:00 300

SATURDAY, 9.6.2011
08:00 Breakfast
09:00 Morning session
09:00 **Martin Plesch:** Encryption with weakly random keys using a quantum ciphertext
09:25 **Matej Pivoluska:** Security of QKD with imperfect sources
09.50 Break & Refreshment
10:15 **Teiko Heinosaari:** Short Tutorial - Invitation to quantum measurements
11:00 **Juha-Pekka Pellonpää:** Extreme quantum instruments and measurement theory
11:25 **Michal Sedlák:** Memory cost of quantum protocols
11:50 End of session
12:00 Lunch
13:30 TRIP visit of Cave Driny and (optional) hike to Zaruby summit
18:30 **Mark Hillery:** Quantum Machines - a Strange History
19:15 CONFERENCE DINNER

SUNDAY, 10.6.2012
08:00 Breakfast
09:00 Morning session
09:00 **Valentin Murg:** The Algebraic Bethe Ansatz and Tensor Networks
09:25 **Barbara Kraus:** Compressed Quantum Simulation of the Ising Model
09:50 Break & Refreshment
10:10 **Miloslav Dušek:** Linear-optical quantum information processing: Recent experiments
10:35 **Enrique Martin-Lopez:** Experimental realisation of Shor's quantum factoring algorithm using qubit recycling
11:00 **Miguel Navascues:** Looking for signs of microscopic quantization
11:25 End of session
11:30 Lunch
12:45 Conference Bus from Smolenice to Bratislava (details will be specified later)

VENUE

The Smolenice Castle was originally built up in the half of 15th century, but it was destroyed during the Rakoci's uprising and Napoleanic wars in 18th century. In 1777 the count Jan Pálffy from Pezinok inherited the entire Smolenice but did not reside in the castle due to its poor condition and lack of money for rebuilding it. The castle was only rebuilt up at the beginning of the 20th century, by order of the count Jozef Pálffy. The architect Jozef Hubert projected the new castle by using the Kreuzenstein castle near Vienna as a model, and the works were controlled by the architect Pavol Reiter from Bavaria. During its construction there were masters from Italy, Germany, Austria and Hungary, and 60 workmen from Smolenice and nearby villages. The main building has two wings and a tower, and is made of ferroconcrete. The castle was damaged again in the spring of 1945 during the World War II, and in that same year the state became its. Smolenice Castle is characteristic by lovely courtyards and beautiful surrounding panorama. Since 1953 it has been housing the Slovak Academy of Sciences and serves as its congress centre, which host yearly thousands of researchers.

The whole castle (except for a few “poshy” rooms) is reserved for CEQIP participants, so feel free to enjoy its atmosphere for informal discussions.

INTERNET
- the wireless network is open and no password required

CURIOSITY
Inventor of the parachute **Štefan Banič** was borned and died in Smolenice. Having witnessed a plane crash in 1912, Banič constructed a prototype of a (military) parachute in 1913. He donated his patent to U.S.Army. It was the first parachute known to be actively used, saving the lives of many U.S. Air Force aviators during World War I.

SOCIAL PROGRAM

WELCOME DINNER
- reception with a selection of delicious food and wine tasting

SOCIAL DINNER
- (Slovak) duck evening with wine

CONFERENCE DINNER
- roasted pig and beers in the outcourt

CONFERENCE TRIP
- cave Driny plus hike to highest summit of the local mountains (approx. 2 hours), or short walk through forrest back to the castle (approx. 1 hour). Let's hope the weather will be nice. Please keep in mind that temperature inside the cave is plus 7,1 – 7,8°C. The cave tour takes approximatively 35 minutes.

CIPHER GAME
Please read carefully! Why? Because only this text could help you to successfully finish the cipher game.

About the game:
We will start on Friday during the dinner, when the ciphers will be distributed. Your first task is to form a team, invent a name of your team and decide on the team leader. The only official role of team leader is to register the team. **Registration will start at 19:00 at the reception**. The team must contain at least three members. The recommended number of team members is 4. Each team will receive an envelope (do not open before 19:30) and a basic cipher-analysis equipment consisting of transformation tables between different representations of English characters (such as Morse code, Braille code, decimal code, binary code, semaphore alphabet, etc.) and also some other valuable information that could be useful for the game. Please do keep the record of the starting times for each cipher, because this information will be used to make formal (and quite irrelevant) order of teams.

The game starts on Friday 19:30. At this time you are allowed to open the envelopes and start solving the first puzzle. The main rule is that teams are not allowed to collaborate. You should do your best to hide your solutions from other teams. Let them find their own answers. It is difficult, but do not shout your solutions and also please minimize any kind of eavesdropping. Solutions point to positions of next puzzles. Altogether the game consists of **7 levels**. Let us stress that the playing per se is more important than the final order. Nevertheless, the winner can be only one. During the first 6 riddles you work as a team. The last one is meant to be solved individually, because there can be only one real winner. Nevertheless, the team is allowed to work jointly also on the last puzzle. The main prize will be given to first individual who correctly reveal the password (being the solution of the last riddle). In case no one will reach the final level before the midnight (we expect this cannot happen), the team which achieves the highest level at first place will obtain all the copies of the final cipher. It is up to this team members whether they want to share the cipher with other teams and give them still some chance to win. At latest the game ends on Saturday evening (we hope this is not going to be the case).

The ciphers are placed inside the castle, or its close (and dark) surroundings. The relevant map will be provided with the first cipher and it is not part of any cipher. Please, pay attention that the positions of the ciphers should not be uncovered for other teams. Always take at most two pieces of the cipher sheets and leave the position of the cipher. From any position you can always return back to the castle and solve the puzzles inside the castle while having some snacks and drinks.

Hint system:
The game should not last longer than by midnight and the hint system should guarantee this. Each cipher contains information on the time when the hints are available. General rule (which is not going to be controlled by anyone) is that you should not ask for the hint sooner than 20 minutes after you reached the cipher (even if help time has already passed). You could ask for the hint also in the case when you already spent more than 50 minutes on it (even if the help time is not reached yet). For the first 4 puzzles you can ask for the “absolute” hint. The hints will be available at the reception (you must bring the cipher with you) and the “absolute” ones for puzzles 1-4 will be slowly presented (if needed) at 20:30, 21:30, 22:30, 23:30, respectively, somewhere in front of the reception. Clear?

Solutions to website ciphers:

Step 1

P	I	Q	E
C	R	O	F
R	E	T	S
I	G	E	R

TO VISIT **Step 2**

Step 3

MASTER **N**EPTUN **C**ANADA
PURPLE **G**ALIUM **T**URTLE

AND **Step 4**

$\sqrt{49}$ 101 5x4 3x3x2 $\sqrt[3]{125}$
cos(0) 100 5^2 3! $0.15x10^2$ 10010

Step 5

captain in panic
hopes evaporate rapidly
google a magic eye

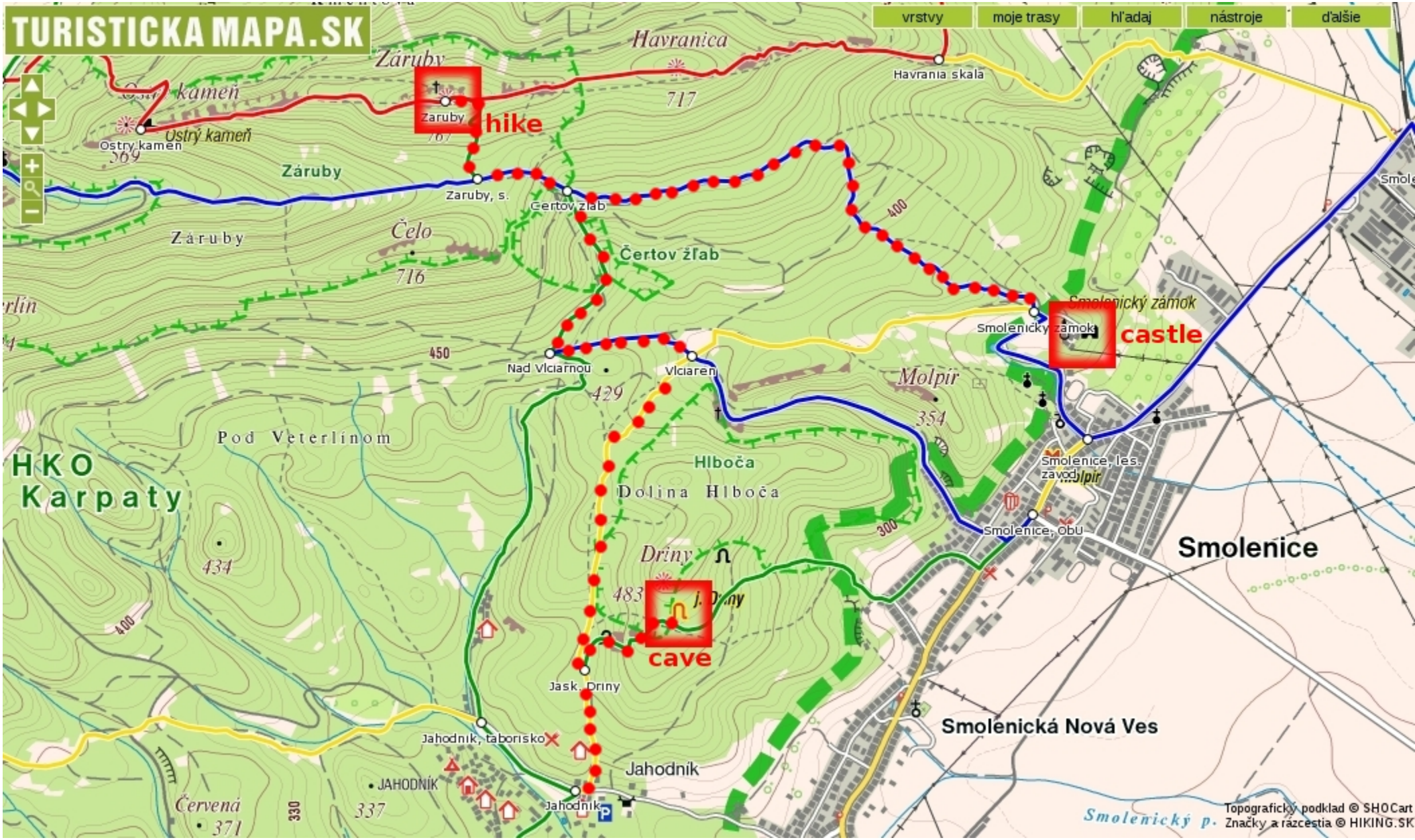
Step 6

CosOexeeRarraSiiiiEurMhoooOuDrE

Step 1 – Start reading from right bottom corner. The solution is *REGISTER FOR CEQIP* . Take home message: be quantum and read in all directions.
Step 2 – You see *ssS*, *mole*, *N*, and *ice*. Putting together *SMOLENICE* (place of the conference). This one could be difficult, because Smolenice is not an English word. All the ciphers are in English, but some local non-English names could appear.
Step 3 – You see six words with six characters each. Clearly 6x6 square, but how to order the word? Why the first characters are in bold? Alphabetically order the words and read the diagonal. If you do not see *CASTLE*, then check that your English alphabet is ABCDEFGHIJKLMNOPQRSTUVWXYZ. This order and the fact that there are 26 characters is very important.
Step 4 – Just transform the expressions into decimals. All of them are between 1 and 26 just as the number of letters in the alphabet. Representing the numbers by the characters gives *GET READY FOR.*
Step 5 – Relatively nonsense text. Always check the simplest encodings. Read just the first letters of those words. You understand why the text is senseless? Because of the *CIPHER GAME*.
Step 6 – Again a nonsense. Small letters separated by capital letters. Can you read CORSE MODE? Almost the Morse code. But how? You need to find two families of symbols representing dots and dashes forming the standard representation of the Morse code. In between the capital letters there are (the same) vowels and consonants. So vowels are dots and consonants are dashes. Or the other way round? The solution is *ALPHABET*, hence, the Morse code could be an example of CEQIP alphabet in which the solutions of the ciphers could be written.

Summing up the steps together: *REGISTER FOR CEQIP* to visit *SMOLENICE CASTLE* and *GET READY FOR CIPHER GAME* and ceqip *ALPHABET*.

Important is that the ciphers are meant to be solved. It is quite easy to make an unbreakable cipher, but this is not our aim. Do not panic when you see the cipher. Just open your mind and relax. You know about Netwon's laws, Fokker-Planck equations, Heisenberg's uncertainty relations, Pauli exclusion principle, Shannon's information, Hund's rules, Turing machines, Bose-Einstein statistics, Mendeleev periodic table of elements, Feynman diagramms, Grover's search algorithms, etc. So there should not be any problem to break some ciphers although there is no general receipt available. Read carefully everything what is on the paper. Not everything is of use, but for sure there are some hidden hints. Help time is really irrelevant. Take into account the fact that most of the ciphers would be very difficult to break for someone outside of our field. And read carefully again what is written here. Have fun! It's just a game.


TURISTICKA MAPA.SK
vrstvy
moje trasy
hľadaj
nástroje
ďalšie
Havranica
717
Záruby
Ostrý kameň
Ostrý kameň
Zaruby
hike
Záruby
Zaruby, s.
Čertov žľab
Čertov žľab
Čelo
716
Záruby
400
Smolenický zámok
Smolenický zámok
castle
Havrania skála
450
Nad Vlciarnou
Vlciareň
429
Molpír
354
Pod Veterlínom
HKO
Karpaty
Hlboča
Dolina Hlboča
Smolenice, les. závod Molpír
Smolenice, OBU
300
Smolenice
Driny
483
cave
434
400
Jask. Driny
Jahodník, taborisko
Smolenická Nová Ves
Jahodník
JAHODNÍK
Jahodník
Červená
371
330
337
Smolenický p.
Topografický podklad © SHOCart
Značky a rázcestia © HIKING.SK