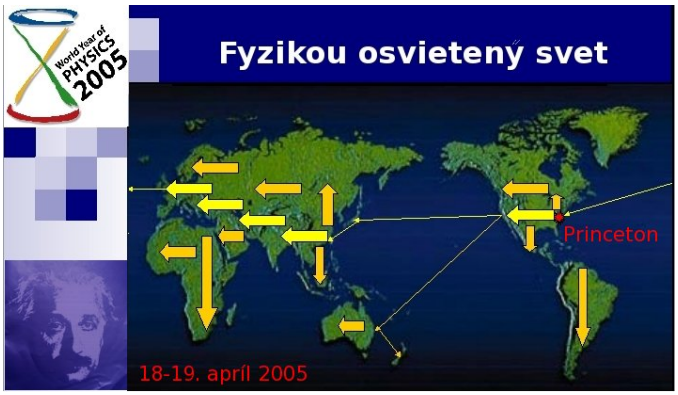
Fyzikou osvietený svet, alebo kryptografia na hraniciach.

Na počesť 50.výročia úmrtia *Alberta Einsteina* sa 18.apríla v americkom meste Princeton svetlo vydalo na svoju púť okolo Zeme. Svetelný signál prešiel na západné americké pobrežie, odtiaľ sa transpacifickým optickým káblom preniesol na pobrežie východnej Ázie. Následne sa signál rozdelil a prešiel severnou a južnou cestou cez Áziu a Európu. Spojil sa v Nemecku, odkiaľ bol poslaný cez Francúzsko a Belgicko do Veľkej Británie. Optickým káblom popod Atlantický oceán sa po 24 hodinovej púti nakoniec vrátil späť do amerického Princetonu. Okrem tejto hlavnej trasy vyslané svetlo precestovalo aj ostatné krajiny. Dostalo sa do krajín Austrálie, Afriky a Južnej Ameriky. Celej tejto akcie s názvom *Fyzikou osvietený svet* (z angl. *Physics enlightens the world*) sa zúčastnilo dovedna 83 krajín a Slovensko nebolo výnimkou.



Obr.1. *Fyzikou osvietený svet.*

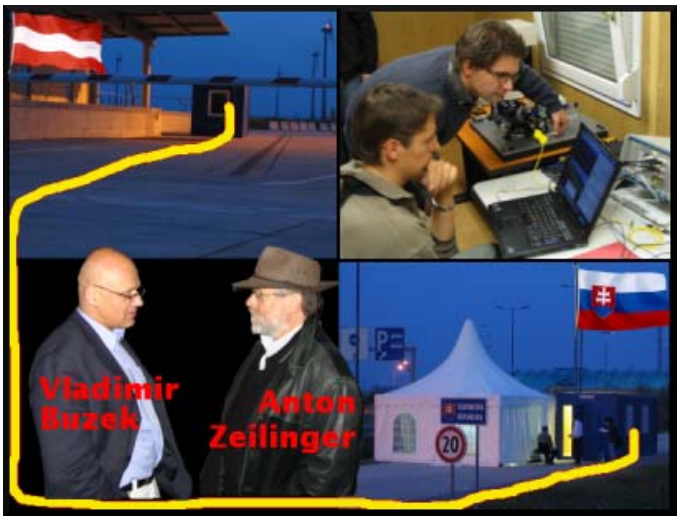
V Bratislave na Fakulte matematiky, fyziky a informatiky Univerzity Komenského sa pri tejto príležitosti uskutočnila séria populárnych prednášok. Vo večerných hodinách o 22:30 táto akcia vyvrcholila vystrelením svetlice, ktorá svetelný lúč posunula o kus dalej. Na slovensko-rakúskej hranici na tento signál čakala skupina fyzikov, ktorí pomocou fotónov svetla preniesli správu *"Physics enligtens the world"* do Rakúska. Išlo o svetovo prvý prenos informácie medzi dvoma štátmi, pri ktorom bola využitá tzv. *kvantová kryptografia*. Písali sme o nej v *Quarku 2005/04*. Na tomto experimente spolupracovala experimentálna skupina profesora *Antona Zeilingera* z Viedenskej univerzity a teoretická skupina profesora *Vladimíra Bužeka* z Fyzikálneho ústavu SAV. Podla ich vlastných slov tento experiment dosvedčil, že celé kryptografické zariadenie nie je dnes obmedzené iba na laboratórne podmienky.

O čo išlo v experimente?

Cieľom experimentu bolo demonštrovať praktické využitie kvantovej fyziky v oblasti fyzike zdanlivo vzdialenej, a síce v kryptografii. Pri kryptografii ide o tajné prenesenie informácie. Môžeme si to predstaviť nasledovne. Odosielateľ napíše správu na papier, ktorý vloží do trezoru a zamkne. Takto uzamknutý trezor pošleme prijímateľovi. Ak chceme preniesť informáciu bezpečne, tak odosielateľ a aj prijímateľ musia vlastniť rovnaký kľúč, pretože iba ten, kto má ten správny kľúč, môže trezor otvoriť. Problémom však je ako tieto kľúče bezpečne rozdistribuovať. Práve k tomuto nám slúžia kvantové systémy. Úlohu kľúča a správy pri modernej komunikácii nahradili reťazce bitov informácie, t.j. postupnosti núl a jednotiek. Proces uzamknutia správy je vykonaný operáciou sčítania kľúča a správy (napr. 11111111), t.j. 00101100+11111111=11010011. Sčitujeme bit po bite pričom platí 0+0=1+1=0, 0+1=1+0=1. Odomknutie vykonáme tým istým postupom, t.j. 11010011+11111111= 00101100. Podobne ako predtým, ten kto nepozná reťazec predstavujúci kľúč, nemá šancu zistiť poslanú správu, resp. Každá správa je roznako pravdepodobná. Problémom je bezpečne rozdistribuovať medzi komunikujúce strany tú istú postupnosť bitov reprezentujúcich kľúč.

Za týmto účelom boli na slovenskej strane generované dvojice fotónov s veľmi špecifickou vlastnosťou typickou iba pre kvantové objekty. Nech sú akokoľvek vzdialené, správajú sa "rovnako". Ak jeden z nich prejde, resp. neprejde, polarizátorom nastavenom v istom smere, tak aj druhý fotón s istotou prejde, resp. s istotou neprejde, polarizátorom nastavenom v tom istom smere. Na voľbe smeru pritom vôbec nezáleží a my hovoríme, že takéto fotóny sú *kvantovo previazané*. Obidve strany obdržia jeden z fotónov a náhodne nastavujú svoje polarizátory. Sledujú, či ich fotón prešiel, alebo nie. Ak fotón prešiel, tak si zanamenajú bit s hodnotou 1 a ak neprešiel, tak majú bit s hodnotou 0. Vdaka vzájomnému previazaniu je výsledok pozorovania, t.j. zaznamenaný bit, taký istý v prípade, ak boli polarizátory nastavené rovnako. Ak je nastavenie rôzne, tak zhoda výsledkov čisto náhodná. V daľšom kroku je preto potrebné odstrániť všetky tie bity, ktoré nezodpovedajú rovnako nastaveným polarizátorom. K tomuto sa použije tzv. verejná komunikácia (napr. telefón), ktorú môže hocikto počúvať. Obidve strany zverejnia smery v akých nastavili svoje polarizátory. Ponechajú si iba tie bity, ktoré boli získané z rovnako nastavených polarizátorov. Tieto sú úplne rovnaké na obidvoch stranách a vytvoria šifrovací kľúč, ktorý sa použije na zakódovanie samotnej správy. O bezpečnosť sa v tomto experimente postarali princípy kvantovej fyziky, t.j. prírodné zákony.

V samotnom experimente bolo potrebné vygenerovať kľúč pozostávajúci z 27 bajtov, t.j. 27x8=216 bitov, pretože prenášaná správa obsahovala 27 znakov. Ak sa však chceme zbaviť akýchkoľvek pochybností o možnom odchytení správy, tak vygenerujeme väčší kľúč a časť z neho si obidve strany porovnajú. Ak sa nájde priveľa chýb, tak celý reťazec bitov zahodíme a začneme generovať odznova. Ak je počet chýb relatívne malý, tak vieme tieto chyby opraviť, resp. komunikáciu vieme "vyčistiť" pomocou klasicky známych postupov na zvýšenie bezpečnosti. Všetky tieto kroky v komunikácii sa prirodzene vykonávajú na počítačoch, ktoré sú v porovnaní s nami predsa len rýchlejšie. Po zadaní správy, ktorú chceme poslať, sa odhadne počet bitov, ktoré je potrebné vygenerovať, aby sme ju celú vedeli zašifrovať. Následne vytvoríme a rozpošleme dvojice fotónov a premeriavame polarizáciu pokiaľ nedostaneme potrebný počet bitov. Z týchto bitov bol nakoniec vyextrahovaný šifrovací kľúč a svetelná štafeta "*Physics enlightens the world*" bola utajene ovzdaná Rakúsku.



Obr. 2. *Prenos štafety do Rakúska. Na obrázku sú odfotené obidve stanice, medzi ktorými bola prenesená správa "Physics enlightens the world". Vzdialenosť medzi stanicami bola zhruba 50 metrov. Vľavo dole s hlavný organizátori celého experimentu: prof. VladimírBužek a prof. Anton Zeilinger. Vpravo hore je samotné experimentálne zariadenie použité na vygenerovanie previazaného páru fotónov, ktoré umožnili distribúciu šifrovacieho kľúča.*

Pocta Einsteinovi

Svetelná štafeta mala za cieľ si pripomenúť 50. výročie bezpochyby jedného z najväčších mysliteľov minulého storočia *Alberta Einsteina,* ktorý posledné roky svojho života prežil práve v americkom Princetone. V roku 1905 Albert Einstein publikoval päť prevratných fyzikálnych prác, ktoré v mnohom zmenili naše nazeranie na svet. Na oslavu tohoto *"zázračného roka"* (*annus mirabilis*) je tento rok vyhlásený za medzinárodný rok fyziky. V jednom roku vysvetlil Brownov pohyb, fotoelektrický jav a sformuloval špeciálnu teóriu relativity. Každý z týchto výsledkov by si zaslúžil Nobelovu cenu, ktorú nakoniec dostal v roku 1921 za fotoelektrický jav, ktorý viedol k neskoršiemu rozvoju kvantovej mechaniky.

Istým paradoxom sa môže zdať, že v kryptografickom experimente na hraniciach bola využitá práve tá vlastnosť kvantovej fyziky, ktorá v Einsteinovi vzbudzovala asi najväčšie pochybnosti. Rozdistribuovanie kľúča využíva jav, ktorý Einstein, Podolski a Rosen vo svojom spoločnom článku označili ako paradoxný. *EPR paradox* však obsahuje hlbokú myšlienku, ktorá v konečnom dôsledku posunula kvantovú fyziku o kus ďalej a je predmetom vedeckých diskusií aj v súčasnosti.

MARIO ZIMAN