**Światełko w tunelu – czyli kwantowy wymiar bezpieczeństwa informacji**

**Doniesienia o groźnych atakach hakerskich i o wyciekach poufnych danych budzić mogą w społeczeństwie informacyjnym coraz większy niepokój. W kontekście rozwoju nowych modeli obliczeniowych i perspektywy budowy komputera kwantowego, klasyczne szyfry kryptograficzne przestają gwarantować bezpieczeństwo. Alternatywę dla tradycyjnie stosowanych metod szyfrowania poufnych informacji oferuje kryptografia kwantowa, wkraczająca na światowy rynek bezpieczeństwa informatycznego.**

Kryptografia kwantowa to pierwsza w historii teoretycznie absolutnie (tj. bezwarunkowo) bezpieczna metoda zapewniania poufności informacji, która może wkrótce znaleźć specjalistyczne zastosowanie na rynku telekomunikacyjnym, jak również pomóc lepiej zabezpieczyć kluczowe łącza administracji publicznej, wojska i ważnych instytucji finansowych. Do bezpiecznej dystrybucji symetrycznego klucza kryptograficznego wykorzystuje ona nanoskopową, kwantową wielkość fizyczną (np. polaryzację pojedynczego fotonu), podlegającą prawom mechaniki kwantowej. Ten sam zupełnie losowo wygenerowany klucz służy do szyfrowania i deszyfrowania informacji w oparciu o szyfr One-time Pad gwarantując kryptosystem komunikacji P2P niepodatny na żadne ataki zewnętrzne. Wygenerowany klucz jest rozdystrybuowany kwantowo za pośrednictwem zwykłego łącza światłowodowego, gdzie propagowany jest stan kwantowy niemożliwy do zmierzenia bez wprowadzenia zaburzeń.

**Bezpieczeństwo na wagę złota**

 O znaczącym potencjale nowej metody szyfrowania danych świadczą komercyjne analizy rynkowe. Według raportu analitycznego GIA i Frost&Sulliva wartość rynkowa kryptografii kwantowej w 2015 osiągnie blisko 842 milionów dolarów. Analitycy Global Industry Analysys, Inc. uważają, że do 2018 rynek ten będzie wart znacznie ponad miliard dolarów. Wśród istotnych graczy zainteresowanych szyfrowaniem kwantowym wymieniają między innymi IDQuantique SA, MagiQ Technologies Inc., Alcatel-Lucent SA, BBN Technologies, HP Laboratories, Infineon Technologies AG, International Business Machines Corp., Nippon Telegraph and Telephone Corp., QinetiQ Group PLC, SPYRUS Inc. i Toshiba.  Skąd bierze się, aż takie zainteresowanie tą technologią? Ważną przesłanką na rzecz wdrażania QKD stanowią zaawansowane obecnie prace nad budową w pełni funkcjonalnego komputera kwantowego, który będzie potrafił w czasie rzeczywistym łamać obecnie stosowane szyfry informatyczne. Klasyczne kryptosystemy opierające się na matematycznych problemach trudnych zostaną wówczas zakwestionowane, jako że problemy te będą mogły być skutecznie rozwiązane przez komputery kwantowe. Wiąże się z tym coraz szerzej dostrzegane zagrożenie dla rozmaitych zabezpieczeń komunikacji o kluczowej roli dla instytucji sektora finansów i bankowości, administracji i wojska. Przełomy technologiczne w tej dziedzinie mają miejsce właśnie obecnie. W maju 2013 roku NASA i Google we wspólnym przedsięwzięciu wdrożyły 512 qubitowe nadprzewodzące komputery kwantowe D-Wave Two drugiej generacji, tworząc pierwsze na świecie kwantowe laboratorium sztucznej inteligencji  (<http://www.youtube.com/watch?v=CMdHDH>).

**Na progu rewolucji**

Wraz z nastaniem ery technologii kwantowych protokoły bezpieczeństwa oparte o złożone problemy matematyczne nie będą już w stanie gwarantować bezpieczeństwa.Jedynym pewnym zabezpieczeniem będą wówczas metody oparte o zasady mechaniki kwantowej. Prace dotyczące komercjalizacji szyfrowania kwantowego są dziś prowadzone w ośrodkach badawczych na całym świecie. Pierwsze komercyjne urządzenia QKD przeznaczone do użytku w standardowych sieciach telco oferują firmy MagicQ Technologies i IDQuantique S.A. Urządzenia obu firm funkcjonują w oparciu o metodę bezsplątaniową. Nie wykorzystują one efektu splątania kwantowego, które powoduje nielokalne korelacje (tj. związki statystyczne) własności fizycznych, stanowiących podstawę dla technologii takich jak teleportacja kwantowa QT czy też bezpieczna kwantowa bezpośrednia komunikacja QSDC (w której komunikowana informacja nie jest przesyłana fizycznie kanałem komunikacyjnym, a proces komunikacji odbywa się w sensie fizycznym nielokalnie, właśnie za pośrednictwem splątania kwantowego). Zjawisko splątania kwantowego wykorzystywane jest jak do tej pory w zaawansowanych prototypowych systemach kryptografii kwantowej rozwijanych np. przez Austrian Institute of Technology (AIT) w Wiedniu, ale także przez NLTK/LFPPI/PWr/CompSecur/seQre we Wrocławiu. Pierwsze  bezsplątaniowe systemy QKD posiadały w swoich prototypowych wersjach wady implementacyjne, pozwalające na przeprowadzenie pewnych klas ataków, jak również charakteryzowały się ograniczoną wydajnością dystrybucji bezpiecznego klucza. Problemy te zostały w ostatnich latach zażegnane, dzięki czemu model bezsplątaniowy znalazł już praktyczne zastosowanie w obszarach zabezpieczania centrów archiwizacji i weryfikacji danych transakcji bankowych RTGS wdrożonych w USA, Japonii, Szwajcarii, Luksemburgu, Austrii, Niemczech i innych krajach UE.

**Kwantowa pieczęć**

Splątaniowa metoda szyfrowania kwantowego wykorzystuje splątanie kwantowe fotonów tworzone w nieliniowym procesie optycznym, w krysztale typu BBO w ramach efektu SPDC (spontaneous parametric down-conversion). Prototypowe splątaniowe systemy poufnej komunikacji odbiorcy z nadawcą integrują wysoce precyzyjne urządzenia optyki kwantowej. W ich skład wchodzą między innymi detektory pojedynczych fotonów oparte na diodach lawinowych, zestawy zintegrowanych silnie tłumionych laserów stanowiących źródła pojedynczych fotonów oraz zaawansowane elektroniczne układy sterujące i bardzo precyzyjne komponenty optyczne.  Rozwijana metoda szyfrowania kwantowego w oparciu o splątanie kwantowe na Politechnice Wrocławskiej w ramach konsorcjum naukowo-badawczego NLTK/LFPPI/PWr./CompSecur/seQre we współpracy z Austriackim Instytutem Technologicznym w Wiedniu zakończyła się wdrożeniem jednej z pierwszych na świecie sieci kwantowych QKD częściowo opartych o splątanie (poza Wrocławiem podobne sieci funkcjonują jeszcze w Wiedniu i w Tokio).

Badania nad nowoczesnymi rozwiązaniami kryptograficznymi mają znaczenie nie tylko dla komercyjnych systemów bezpieczeństwa. Innowacyjna metoda szyfrowania kwantowego, szczególnie splątaniowego może korzystnie wpłynąć na sytuację strategiczną Polski na arenie międzynarodowej, a w wymiarze ekonomicznym znacznie podnieść jej znaczenie w obszarze high-techu. Upowszechnienie kryptografii kwantowej to jak pokazują prognozy nie kwestia dekad, lecz kilku najbliższych lat. Prawdopodobnie już wkrótce zabezpieczenia oparte o procedury oparte na prawach mechaniki kwantowej zagwarantują w specjalistycznych zastosowaniach, wdrażanych także na rynku krajowym, teoretycznie bezwarunkowy poziom poufności informacji, który jak do tej pory był poza zasięgiem.

Firma CompSecur i jej spin-off seQre są współorganizatorami unikalnego w skali międzynarodowej V Sympozjum LFPPI seQre2014: Progress in Quantum Cryptography, które odbędzie się na Politechnice Wrocławskiej w dniach 27-28 stycznia 2014 roku. Serdecznie zapraszamy zainteresowanych do udziału w Sympozjum.

Firma CompSecur oraz jej spin-off seQre, prowadzą szereg projektów badawczo-rozwojowych w zakresie komercjalizacji systemów kryptografii kwantowej. Są współorganizatorami V Sympozjum LFPPI seQre 2014 Progress in Quantum Cryptography. Współpracują z Polską Agencją Rozwoju Przedsiębiorczości oraz siecią naukową KBN Laboratorium Fizycznych Podstaw Przetwarzania Informacji LFPPI i Narodowym Laboratorium Technologii Kwantowych NLTK. Jako jedyne firmy w Polsce zajmują się bezpieczeństwem przesyłania danych z wykorzystaniem kryptografii kwantowej. Wraz z LFPPI, NLTK i Politechniką Wrocławską oraz Austriackim Instytutem Technologicznym w Wiedniu, prowadzą zaawansowane badania w zakresie technologii splątania kwantowego.

CompSecur sp. z o.o.
email: info@compsecur.pl
<http://seqre.net/seqre2014/>

