MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
PROGRAMMI DI RICERCA - ANNO 2005

COMPITI E SUDDIVISIONE FONDI TRA LE UNITÀ DI RICERCA
prot. 2005024981

Coordinatore Scientifico	Giacomo Mauro D'ARIANO
Ateneo	Università degli Studi di PAVIA
Titolo della Ricerca	Distribuzione di informazione quantistica e crittografia
Finanziamento assegnato	**Euro** 237.000
Durata	24 Mesi

Obiettivo della Ricerca

Il principale obiettivo del presente progetto di ricerca è lo studio della distribuzione di informazione quantistica, da entrambi i punti di vista, teorico e sperimentale, analizzando i limiti di principio alla realizzabilità, e implementando una nuova tecnologia per il bradcasting quantistico. In particolare, si analizzarà accuratamente la possibilità di purificare gli stati durante la distribuzione---il cosiddetto "super-bradcasting"---valutando le correlazioni tra i vari utenti e derivando i trade-off tra sicurezza e broadcasting nel caso in cui il protocollo di broadcasting sia utilizzato per distribuire quantisticamente chiavi crittografiche. All'interno del programma verrano anche studiati nuovi schemi crittografici recentemente proposti---più efficaci contro intercettamenti e interazioni con l'ambiente circostante--- insieme a tecniche di intercettazione ed il relativo trade-off tra informazione e disturbo. Saranno migliorate alcune tecnologie applicate nell'ottica quantistica, tra cui schemi più efficienti di ottica non-lineare, tecniche per ridurre il rumore, generazione di nuove sorgenti e migliori detector.

Il progetto coinvolgerà il gruppo teorico di Pavia e quello sperimentale di Roma in una stretta collaborazione.

In considerazione del taglio considerevole nel cofinanziamento di circa il 42% che ridurrà del 50% il personale postdoc, si prevede di portare avanti solo alcune delle linee di ricerca previste dal progetto. In particolare, saranno oggetto di eventuali progetti finanziati da altri enti le linee teoriche sulla parte di crittografia (analisi crittografiche e il trade-off informazione disturbo, nonchè lo studio di nuovi schemi crittografici), nonchè l'obiettivo sperimentale della ricerca di nuove sorgenti di informazione quantistica, comprendendo in particolare la generazione e la caratterizzazione di stati "bound entangled".

Innovazione rispetto allo stato dell'arte nel campo

Il progetto di ricerca è particolarmente innovativo, in quanto rivolto all'argomento del broadcasting di informazione, che allo stato attuale costituisce un'area non ancora sviluppata nel campo dell'Informazione Quantistica. La realizzazione del progetto è basata sulla sinergia fra due gruppi---uno teorico e l'altro sperimentale---che esprimono un livello di eccellenza notevole all'interno del panorama internazionale, e collaborano con i principali gruppi, sia europei che extraeuropei, attivi nel settore. La proposta è orientata all'ideazione di dispositivi che sarranno utili alla comunità scientifica e che si ritengono realizzabili nella durata di due anni con le attuali tecnologie e conoscenze. Tali dispositivi avranno un notevole impatto tecnologico a lungo termine e saranno di utilità più immediata dal lato puramente scientifico.

L'impatto potenziale della tecnologia dell'informazione quantistica è vasto e significativo. Il presente progetto è fondato su una serie di ricerche sperimentali e teoriche per lo sviluppo di nuovi dispositivi ottici, metodi teorici per progettare e ottimizzare tali dispositivi, coinvolgendo scienziati con alta qualificazione a livello internazionale. Il progetto porterà un notevole beneficio socio-formativo, in quanto permetterà di coordinare differenti attività di ricerca scientifica e tecnologica in uno sforzo mirato, in modo da mantenere l'Italia ad un alto livello di eccellenza internazionale, e da rinvigorire la competitività italiana. L'area di ricerca dell'Informazione Quantistica è in continuo sviluppo e si ritiene che aumenterà ancora di importanza nel breve periodo grazie a una nuova serie di attività scientifiche e tecnologiche. Per questa ragione è necessario sviluppare un polo italiano di competenze e conoscenze che sia in grado di fare fruttare il potenziale a lungo termine del settore, e di introdurre nel contesto internazionale, sia scientifico che industriale, il proprio contributo di innovazioni tecnologiche. Infine, la pubblicizzazione dei risultati ottenuti e le attività di formazione previste del progetto rappresentano un importante contributo all'arricchimento di conoscenza della comunità scientifica.

RECENTI SVILUPPI SUCCESSIVI ALLA SOTTOMISSIONE DEL PROGETTO

Recenti risultati teorici suggeriscono di considerare metodi di Teoria Quantistica di Campo e Topologici per lo studio sistematico del broadcasting quantistico. Per questo si prevede di investire rilevanti risorse nello sviluppo di tali metodologie, in collaborazione con il prof. L. Kauffman dell'University of Illinois di Chicago e con ricercatori del forum internazionale LQP (Local Quantum Physics), in particolare con il gruppo di Amburgo (prof. R. Haag) e con il gruppo di Sendai in Giappone (prof. M. Ozawa). In particolare si prevede di organizzare la prima conferenza internazionale di Quantum Field Theory of Measurements, portando a convergenza competenze teoriche complementari, dalla teoria algebrica di campo, metodi topologici, sistemi quantistici aperti, quantum information e fondamenti della meccanica quantistica (in particolare Interpretazione Modale).

Criteri di verificabilità

Oltre che dalla realizzazione dei dispositivi sperimentali proposti, che in conclusione potrebbe portare a dei brevetti, i criteri suggeriti per la certificazione della qualità e del raggiungimento degli obbiettivi di questo progetto sono le pubblicazioni su riviste scientifiche di prestigio internazionale passate al vaglio di referees, i libri, gli articoli di rassegna su invito e la partecipazione su invito a conferenze internazionali.

Elenco delle Unità di Ricerca

Sede dell'Unità	Università degli Studi di PAVIA
Responsabile Scientifico	Giacomo Mauro D'ARIANO
Finanziamento assegnato	**Euro** 109.000

Compito dell'Unità

Il gruppo di Pavia si occuperà delle linee di ricerca teoriche, e coadiuverà il gruppo di Roma nella fase di progettazione degli esperimenti proposti, e nell'analisi numerica dei dati. Gli obbiettivi principali includeranno, da una parte, una completa caratterizzazione dei diversi metodi di distribuire informazione quantistica, con il proposito di ideare opportuni schemi sperimentali, e dall'altra, un'analisi della tecnologia attualmente disponibile, valutata in rapporto agli schemi ottimi ricavati teoricamente. È inoltre in programma un'analisi dettagliata delle correlazioni presenti fra vari utenti negli schemi di distribuzione di informazione quantistica.

Considerato il taglio del 42% del cofinanziamento (che produrrà un taglio effettivo del 50% del personale postdoc), sarà oggetto di un diverso progetto finanziato da altri enti la parte di crittografia quantistica del progetto cofinanziato, comprendente analisi di sicurezza e derivazione del tradeoff fra sicurezza e broadcasting, nonchè l'ideazione di nuovi protocolli crittografici basati su qudit (stati a dimensionalità maggiore di due).

D'altro canto, recenti risultati teorici suggeriscono di considerare metodi di Teoria Quantistica di Campo e Topologici per lo studio sistematico del broadcasting quantistico. Per questo si prevede di investire rilevanti risorse nello sviluppo di tali metodologie, in collaborazione con il prof. L. Kauffman dell'University of Illinois di Chicago e con ricercatori del forum internazionale LQP (Local Quantum Physics), in particolare con il gruppo di Amburgo (prof. R. Haag) e con il gruppo di Sendai in Giappone (prof. M. Ozawa). In particolare si prevede di organizzare la prima conferenza internazionale di Quantum Field Theory of Measurements, portando a convergenza competenze teoriche complementari, dalla teoria algebrica di campo, metodi topologici, sistemi quantistici aperti, quantum information e fondamenti della meccanica quantistica (in particolare Interpretazione Modale).

Sede dell'Unità	Università degli Studi di ROMA "La Sapienza"
Responsabile Scientifico	Francesco DE MARTINI
Finanziamento assegnato	**Euro** 128.000

Compito dell'Unità

Il gruppo di Roma si occuperà della realizzazione sperimentale dei canali di broadcasting, utilizzandoli poi per diversi scopi, quali la riduzione del rumore, e l'applicazione a schemi crittografici a molti utenti. Verranno considerati diversi schemi di cloning approssimato al fine di distribuire informazione quantistica, le cui prestazioni saranno analizzate sia teoricamente che sperimentalmente (attraverso il metodo della tomografia quantistica). Ci si occuperà inoltre di studiare le proprietà di sistemi quantistici di dimensione maggiore di due (qutritt/ququart) e le tecniche per la preparazione di stato per applicazioni crittografiche. Verranno ideati nuovi dispositivi sperimentali in grado di raggiungere il limite ottimo del rapporto informazione/disturbo, che saranno basati su tecniche di cloning e teletrasporto, e saranno finalizzati ad un parziale recupero di informazione classica da stati quantistici. Nel corso di questo progetto verranno perfezionate alcune tecniche sperimentali, attraverso l'uso di schemi efficienti di ottica nonlineare basati su cristalli "periodically poled" e/o su nuove configurazioni spaziali e a doppio cristallo, sulla generazione di stati entangled a più fotoni che siano robusti rispetto alle perdite, e, infine, su fibre a singolo modo combinate con rivelatori con una sufficiente risoluzione nel numero di fotoni.

Considerato il taglio del 42% del cofinanziamento (che produrrà un taglio effettivo del 50% del personale postdoc e nell'acquisizione di strumenti), non sarà invece possibile perseguire l'obiettivo previsto della ricerca di nuove sorgenti di informazione quantistica, comprendendo in particolare la generazione e la caratterizzazione di stati "bound entangled".