



## MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA

### Programmi di ricerca cofinanziati - Modello E Relazione scientifica conclusiva sui risultati di ricerca ottenuti - ANNO 2007 prot. 2007FYETBY

<b>1. Area Scientifico Disciplinare principale</b>	09: Ingegneria industriale e dell'informazione
<b>2. Coordinatore Scientifico del programma di ricerca</b>	MONDIN Marina
- Università	Politecnico di TORINO
- Facoltà	Facoltà di INGEGNERIA III
- Dipartimento/Istituto	Dip. ELETTRONICA
<b>3. Titolo del programma di ricerca</b>	Studio di fattibilità della realizzazione di un canale di comunicazione quantistica ottica terra-spazio (CCQOTS)
<b>4. Settore principale del Programma di Ricerca:</b>	ING-INF/03
<b>5. Costo originale del Programma:</b>	350.000 €
<b>6. Quota Cofinanziamento MIUR:</b>	140.000 €
<b>7. Quota Cofinanziamento Ateneo:</b>	60.000 €
<b>8. Finanziamento totale:</b>	200.000 €
<b>9. Durata:</b>	24 mesi

## 10. Obiettivo della ricerca eseguita

La finalità del progetto è stata duplice: da un lato è stato realizzato, grazie alla sinergia tra l'unità di Torino e quella di Bologna, un simulatore atmosferico accoppiato ad un protocollo di distribuzione quantistica di una chiave crittografica, dall'altro si è studiata l'applicazione di tecniche di "information reconciliation" espressamente progettate per il caso della trasmissione in questione.

Entrambi gli obiettivi erano finalizzati allo studio di una possibile realizzazione di un canale di comunicazione quantistica terra-spazio, basato su una simulazione realistica seppure con costi limitati, ed in grado di utilizzare le più recenti tecniche di "signal processing".

Gli obiettivi previsti sono stati raggiunti con successo, come dettagliato nella descrizione della ricerca eseguita.

I risultati di carattere scientifico sono inoltre stati disseminati con successo, divulgando la tematica delle comunicazioni quantistiche all'interno della comunità scientifica internazionale storicamente dedita allo studio del processamento del segnale.

## 11. Descrizione della Ricerca eseguita e dei risultati ottenuti

\* Descrizione dell'attività scientifica

Il Progetto si è occupato di trasmissione quantistica a singolo fotone su canale satellitare sicuro ed affidabile per applicazioni di distribuzione di chiave crittografica (Quantum Key Distribution or QKD), e si è articolato in tre fasi, che si sono occupate rispettivamente di (1) Modellizzazione numerica del canale quantistico a singolo fotone, (2) Realizzazione sperimentale del protocollo di comunicazione BB84 su banco ottico con emulatore di canale atmosferico e (3) Analisi di tecniche di "information reconciliation".

L'attività svolta nel corso del Progetto viene qui descritta seguendo tale suddivisione.

(1) Per quanto riguarda la modellizzazione del canale trasmissivo, sono stati costruiti i modelli numerici di differenti condizioni atmosferiche (variabili a seconda dei gas, aerosoli, inquinanti presenti nell'atmosfera) ed è stato analizzato il trasferimento radiativo in funzione della geometria trasmissiva e dei parametri atmosferici. Tale attività ha portato allo sviluppo della pubblicazione congiunta fra le due sedi [1].

(2) Per quanto riguarda lo studio di protocolli di comunicazione per QKD e la loro realizzazione su banco ottico, dopo uno studio preliminare degli stati entangled prodotti in un Photon Counter Detector (PDC) per possibile utilizzo in applicazioni di QKD [2-4,6,7,18], sono stati realizzati due schemi specifici di QKD: uno basato su codifica in spazi di Hilbert pluridimensionali [15,17], l'altro su un protocollo ideato da Vaidamn che considera stati ortogonali [19,22]. È stato inoltre sviluppato un esperimento in grado di valutare gli effetti atmosferici simulati in cella su protocollo QKD, che ha permesso di confrontare i risultati di trasferimento radiativo numerici ottenuti nell'attività (1) con quelli sperimentali ottenuti per emulazione. È stato infine eseguito il test degli effetti atmosferici simulati in cella su un protocollo di QKD (BB84) [1].

(3) Per quanto riguarda l'analisi di tecniche di codifica e signal processing per QKD e l'analisi di tecniche di "information reconciliation" per QKD, sono stati analizzate tre tematiche specifiche, descritte nel seguito:

(3.1) Analisi di codici di canale robusti e ad elevate prestazioni da utilizzare per la protezione della chiave quantistica da possibili errori di trasmissione, (3.2) Analisi di possibili metriche di tipo "soft" per applicazioni di "information reconciliation" e "privacy amplification"

(3.3) Analisi di tecniche di trasmissione e signal processing adatti per la trasmissione sul canale pubblico

(3.1) Nella QKD il mittente codifica l'informazione in stati quantistici trasmessi su un "quantum channel" sicuro, il destinatario li osserva e quindi, dopo una discussione pubblica su un canale pubblico inaffidabile delle loro osservazioni, condividono una parte dell'informazione che è la stessa per entrambi (con una probabilità d'errore arbitrariamente alta). La loro discussione deve poter far fronte anche ad errori che possono essere introdotti dal rumore nel canale di comunicazione o da una spia, ma deve essere tale per cui l'informazione non sia compromessa. Quindi è importante individuare codici di canale robusti e ad elevate prestazioni da utilizzare per la protezione dell'informazione dagli errori in tale contesto [20], problema che è stato affrontato nel corso di questa attività. In alternativa ai cosiddetti "turbo" codici, si sono studiati codici prodotto convoluzionali e codici convoluzionali a concatenazione seriale, per superare un limite riconosciuto dei turbo codici "classici", e cioè la degradazione delle loro prestazioni per tassi molto bassi della probabilità di errore. In particolare, si è considerato il progetto di codici prodotto convoluzionali, anziché di codici prodotto a blocco, e si sono studiati metodi di terminazione e di tail-biting di tali schemi di codifica [9,11]. Si è inoltre intrapreso e concluso lo studio di codici concatenati serialmente in grado di conseguire valori estremamente variabili dell'efficienza spettrale,

ricorrendo alla punturazione dei bit prodotti dal codificatore [5]. In particolare si sono determinati gli effetti indotti dalla punturazione attraverso la messa a punto di modelli che consentono di stimare le prestazioni medie in un contesto in cui il maggior problema è la complessità dell'ottimizzazione (per i molti gradi di libertà che il sistema offre). Si è assunta, come misura delle prestazioni dei codici, il loro tasso d'errore residuo sul bit e sulla parola di codice dopo la decodifica. Si è assunto inoltre di decodificare tali codici utilizzando algoritmi di decodifica iterativa di tipo soft.

(3.2) Al fine affiancare alla informazione sicura ma di tipo "hard" proveniente da un canale quantistico, con quella inaffidabile ma "soft" proveniente dal canale AWGN (Additive White Gaussian Noise) pubblico, nel corso di questa attività è stato proposto l'uso di metriche di tipo "soft" derivate dal "quantum channel" [8,16,21,23], il cui peso è stato ottimizzato in modo da minimizzare il tasso di errore del sistema [10,16]. Tali metriche sono state congiuntamente a codici di tipo Low Density Parity Check (LDPC) decodificati con algoritmi iterativi di tipo "belief propagation", le cui prestazioni sono state analizzate nella pubblicazione [12]. Si noti che le metriche soft considerate prendono in considerazione le non idealità del quantum channel introdotte dalle non idealità dell'atmosfera modellizzate nell'attività (1). Si noti inoltre che i codici per la correzione d'errore considerati offrono tassi di errore molto ridotti, che richiedono, per la loro stima, simulazioni molto lunghe, svolte possibilmente su più computer in parallelo.

(3.3) Una parte dell'attività è stata dedicata allo studio delle prestazioni del canale pubblico ad alta velocità, e delle relative tecniche di trasmissione, finalizzate alla massimizzazione del throughput ed alla minimizzazione del numero di operazioni eseguite. Sono stati proposti a tale scopo una tecnica per il progetto di filtri di decimazione privi di moltiplicatori, e l'uso di tecniche di "fairness" proporzionale, descritte rispettivamente nelle pubblicazioni [13] e [14].

#### \* Pubblicazioni generate dal Progetto

##### Pubblicazioni su riviste a diffusione internazionale

[1] N. Antonietti, M. Mondin, F. Daneshgaran, G. Giovanelli, I. Kostadinov, B. Lunelli, G. Brida, M. Genovese, M. Gramegna; "Quantum bit error rate in modeled atmospheres", *Int. Journ. Quant. Inf.* 7 (2009), 213.

[2] G. Brida, L. Caspani, A. Gatti, M. Genovese, A. Meda, I. Ruo-Berchera, "Measurement of sub-shot-noise spatial correlations without subtraction of background", *Phys. Rev. Lett.* 102, 213602 (2009).

[3] A. Allevi, A. Andreoni, M. Bondani, G. Brida, M. Genovese, M. Gramegna, S. Olivares, M. G. A. Paris, P. Traina, G. Zambra; "State reconstruction by simple measurements"; *Phys. Rev. A* 80 (2009) 022114.

[4] G. Brida, V. Caricato; M. Fedorov, M. Genovese, M. Gramegna, S. Kulik, "Characterization of Spectral Entanglement of Spontaneous Parametric-Down Conversion Biphotons" *EPL* 87 (2009) 64003.

[5] A. Graell i Amat, G. Montorsi and F. Vatta, "Design and performance analysis of a new class of rate-compatible Serial Concatenated Convolutional Codes", *IEEE Transactions on Communications*, Vol. 57, No. 8, August 2009, pp. 2280-2289.

[6] G. Brida, I. Degiovanni, A. Florio, M. Genovese, P. Giorda, A. Meda, M. Paris, Alex Shurupov, "Experimental estimation of entanglement at the quantum limit", *PRL* 104, 100501 (2010).

[7] G. Brida, V. Caricato, M. V. Chekhova, M. Genovese, M. Gramegna, and T. Sh. Iskhakov, "Testing Ultrafast Two-Photon Spectral Amplitudes via Optical Fibres", *Optics Express* Vol. 18 (2010) 12915.

[8] Marina Mondin, Maria Delgado, Fabio Mesiti, Fred Daneshgaran, "Soft-processing for Information Reconciliation in QKD Applications", *International Journal of Quantum Information*, special issue on "Advances in foundations of Quantum Mechanics and Quantum Information", to appear (2010).

##### Atti di congressi internazionali

[9] F. Vatta, V. Sidorenko, and M. Bossert, "Termination and tailbiting of rate-k/n direct product convolutional codes", *Proc. of the 2010 IEEE International Symposium on Information Theory, ISIT'10*, Austin, Texas, U.S.A., June 13 - 18, 2010, pp. 2023-2027.

[10] Marina Mondin, Fred Daneshgaran, Maria Delgado, and Fabio Mesiti, "Soft-metric-based information reconciliation techniques for QKD", in *Proc. SPIE 7815, 781502 (2010)* doi:10.1117/12.858357, *Quantum Communications and Quantum Imaging VIII Conference*, Conference Chairs: Ronald E. Meyers, Yanhua Shih, Keith S. Deacon.

[11] F. Vatta, A. Schiavi, V. Sidorenko, and M. Bossert, "Termination and tailbiting of direct product convolutional codes", *Proc. of the 2009 IEEE Information Theory Workshop, ITW '09*, Taormina, Italy, October 11 - 16, 2009, pp. 213-217.

[12] Daneshgaran, F.; Laddomada, M.; Mondin, M.; "LDPC-Based Iterative Algorithm for Compression of Correlated Sources at Rates Approaching the Slepian-Wolf Bound", *Advances in Satellite and Space Communications*, 2009. SPACOMM 2009, First International Conference on, 20-25 July 2009 Page(s):74 - 79.

[13] Laddomada, M.; Mesiti, F.; Mondin, M.; "Design of multiplierless decimation filters based on Cyclotomic Polynomials", *Circuits and Systems*, 2009. MWSCAS '09. 52nd IEEE International Midwest Symposium on, 2-5 Aug. 2009 Page(s):673 - 678.

[14] Daneshgaran, F.; Laddomada, M.; Mesiti, F.; Mondin, M.; "On the Throughput Allocation for Proportional Fairness in Multirate IEEE 802.11 DCF", *Consumer Communications and Networking Conference*, 2009. CCNC 2009. 6th IEEE, 10-13 Jan. 2009 Page(s):1 - 5.

[15] A.P. Shurupov, G. Brida, I. Degiovanni, M. Genovese, A. Florio, A. Meda, P. Giorda, and M. Paris, "Optimal evaluation of entanglement in two qubit system", *18th International Laser Physics Workshop (LPHYS'09)*, July 13 - 17, 2009, Barcelona, Spain

[16] Mondin M., F. Daneshgaran, M. Delgado, F. Mesiti, "Novel Techniques for Information Reconciliation, Quantum Channel Probing and Link Design for Quantum Key Distribution", in *Proceedings of PSATS 2010*, Roma, Italy, February 2010.

[17] G. Brida, V. Caricato, M. Genovese, M. Gramegna, M.V. Fedorov., S.P. Kulik, "Entanglement Degree Characterization of Spontaneous Parametric-Down Conversion Biphotons in Frequency Domain", *Quantum Communication and Quantum Networking* Publisher, Springer, Berlin Heidelberg, pag.46, A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): *QuantumCom 2009*.

[18] G. Brida, M. Genovese, M. Gramegna, F. Piacentini, S. Olivares, and M. G. A. Paris, "On/off Detection Method for Reconstructing the Statistics of Quantum Optical States: An Overview", *Proceedings ICQNM 2009 - The Third International Conference on Quantum, Nano and Micro Technologies*, 1-7 February 2009 Cancun, Mexico.

[19] A. Avella, G. Brida, I. P. Degiovanni, M. Genovese, M. Gramegna, and P. Traina "Experimental quantum cryptography scheme based on orthogonal states: preliminary results" *Proc. SPIE* Vol. 7702, 77020E (2010).

[20] F. Vatta, R. Romano, and F. Mesiti, "Analysis and design of parallel concatenated channel codes for Quantum Key Distribution (QKD) applications", *Proc. di ISABEL 2010*, Roma, 7-10 Novembre 2010.

[21] Stefano Olivares, Matteo G. A. Paris, Maria Delgado and Marina Mondin "Toward a "soft" output quantum channel via Bayesian estimation", *Proc. di ISABEL 2010*, Roma, 7-10 Novembre 2010.

[22] Alessio Avella, Giorgio Brida, Ivo Pietro Degiovanni, Marco Genovese, Marco Gramegna and Paolo Traina, "Experimental realization of Goldenberg - Vaidman QKD Protocol", *Proc. di ISABEL 2010*, Roma, 7-10 Novembre 2010.

[23] Fabio Mesiti, Fred Daneshgaran, Maria Delgado and Marina Mondin, "Sparse-graph codes for information reconciliation in QKD applications invited paper", *Proc. di ISABEL 2010*, Roma, 7-10 Novembre 2010.

#### \* Attività di disseminazione

1) Organizzazione di una sessione speciale sul Progetto PRIN 2007 "Feasibility study of an optical Earth-satellite quantum communication channel" coordinata da Marina Mondin al congresso "5th Workshop ad memoriam of Carlo Novero, Advances in Foundations of Quantum Mechanics and Quantum Information with atoms and photons", con 3 presentazioni incentrate sulle attività del Progetto.

2) Organizzazione di una sessione speciale su "Quantum communication and Quantum Processing" alla riunione annuale del gruppo GTTI, Brescia, 22 Giugno 2010, con due delle presentazioni dedicate alle attività del Progetto.

3) Organizzazione di una sessione speciale su "Quantum communication and Quantum Key Distribution" all'International Symposium on Applied Sciences in Biomedical and Communication Technologies, ISABEL 2010, Roma, 7-10 Novembre 2010, con 4 invited paper relativi al Progetto, ed in le pubblicazioni [20-23].

I risultati preliminari ottenuti dal Progetto sono inoltre stati presentati al meeting finale del progetto COST 297 "HAPCOS" (Avignone, 16-23 ottobre 2009).

#### \* Partecipazioni a conferenze internazionali

Sempre all'interno dell'attività di disseminazione e di interazione con la comunità scientifica internazionale, il Progetto ha generato la partecipazione alle seguenti conferenze internazionali (ed alla presentazione dei relativi risultati scientifici generati dal Progetto e/o all'interazione con esperti del settore):

1) "18th Intern. LPHYS 2009" Barcellona;

2) "MWSCAS 2009", Messico, 02-05/08/09;

3) "SPACOMM 2009", Francia, 20-25/07/09;

- 4) "IEEE CCNC 2009", Las Vegas, USA, 10-13/01/09;
- 5) "ITW '09", Taormina, Italy, 11-16/10/2009;
- 6) "PSATS 2010", Roma, Italy, February 2010 (2 persone);
- 7) "Quantum 2010, 5th Workshop ad memoriam of Carlo Novero", Torino, Italy, 23-29/5/2010 (5 persone);
- 8) "SPIE Optics + Photonics 2010", San Diego, USA, 1-4/8/2010;
- 9) "IGARRS 2010", Honolulu, USA, 25-30/7/2010;
- 10) "Isabel 2010", Roma, Italy (4 persone, 7-10 novembre 2010).

\* Attività di coordinamento e di interazione con la comunità scientifica

Come previsto, sono state svolte periodiche riunioni di coordinamento fra le sedi, oltre a missioni finalizzate a collaborazioni scientifiche sulle tematiche del Progetto (Padova, Los Angeles, Russia).

\* Addestramento di personale

L'attività sperimentale e di ricerca è stata svolta con il supporto di due assegnisti di ricerca, che sono stati addestrati specificamente per l'attività relativa al Progetto. Si è inoltre usufruito della collaborazione con dottorandi, che sono stati addestrati sulle tematiche del Progetto, anche con la partecipazione a scuole di dottorato e a riunioni scientifiche.

\* Acquisizione di strumentazione

È stata acquisita la seguente strumentazione, finalizzata allo svolgimento del Progetto:

- 1) calcolatori e notebook per l'ottenimento di risultati simulativi e per la presentazione di risultati
- 3) personal computer industriale da laboratorio per il coordinamento delle operazioni di misura
- 4) cristalli non-lineari per banco ottico QKD
- 5) protezione per banco ottico e laser per esperimenti di QKD

\* Esperimenti realizzati o messi in opera

- 1) banco ottico per schema QKD alla Vaidman
- 2) sistema generazione qubits/ququats
- 3) esperimento di effetti atmosferici simulati in cella su protocollo QKD

## 12. Problemi riscontrati nel corso della ricerca

NESSUN PROBLEMA RISCONTRATO

## 13. Risorse umane complessivamente ed effettivamente impegnate (da consuntivo)

	(mesi uomo)
<b>TOTALE</b>	<b>48</b>
<b>da personale universitario</b>	<b>48</b>
<b>altro personale</b>	<b>82</b>
<b>Personale a contratto a carico del PRIN 2007</b>	<b>47</b>

## 14. Modalità di svolgimento (dati complessivi)

### Partecipazioni a convegni:

	Già svolti (numero)	Da svolgere (numero)	Descrizione
<b>in Italia</b>	12	0	Si sono avute 12 partecipazioni in Italia a conferenze su argomenti relativi al Progetto (talvolta con più di un partecipante alla stessa conferenza). Si noti che 4 di queste partecipazioni sono state su invito. Sono inoltre state organizzate due sessioni speciali di conferenze internazionali (svolte in Italia) relative agli argomenti del Progetto, ed una sessione tecnica alla riunione nazionale del gruppo GTTI.
<b>all'estero</b>	7	0	Si sono avute 7 partecipazioni a conferenze all'estero su argomenti relativi al Progetto. Si noti che 2 di queste partecipazioni sono state su invito.
<b>TOTALE</b>	<b>19</b>	<b>0</b>	

Per ogni campo di testo max 8.000 caratteri spazi inclusi

### Articoli pertinenti pubblicati:

	Numero	Descrizione
<b>su riviste italiane con referee</b>	0	

<b>su riviste straniere con referee</b>	8	<p>[1] N. Antonietti, M. Mondin, F. Daneshgaran, G. Giovanelli, I. Kostadinov, B. Lunelli, G. Brida, M. Genovese, M. Gramegna; "Quantum bit error rate in modeled atmospheres", <i>Int. Journ. Quant. Inf.</i> 7 (2009), 213.</p> <p>[2] G. Brida, L. Caspani, A. Gatti, M. Genovese, A. Meda, I. Ruo-Berchera, "Measurement of sub-shot-noise spatial correlations without subtraction of background", <i>Phys. Rev. Lett.</i> 102, 213602 (2009).</p> <p>[3] A. Allevi, A. Andreoni, M. Bondani, G. Brida, M. Genovese, M. Gramegna, S. Olivares, M. G. A. Paris, P. Traina, G. Zambra; "State reconstruction by simple measurements"; <i>Phys. Rev. A</i> 80 (2009) 022114.</p> <p>[4] G. Brida, V. Caricato; M. Fedorov, M. Genovese, M. Gramegna, S. Kulik, "Characterization of Spectral Entanglement of Spontaneous Parametric-Down Conversion Biphotons" <i>EPL</i> 87 (2009) 64003.</p> <p>[5] A. Graell i Amat, G. Montorsi and F. Vatta, "Design and performance analysis of a new class of rate-compatible Serial Concatenated Convolutional Codes", <i>IEEE Transactions on Communications</i>, Vol. 57, No. 8, August 2009, pp. 2280-2289.</p> <p>[6] G. Brida, I. Degiovanni, A. Florio, M. Genovese, P. Giorda, A. Meda, M. Paris, Alex Shurupov, "Experimental estimation of entanglement at the quantum limit", <i>PRL</i> 104, 100501 (2010).</p> <p>[7] G. Brida, V. Caricato, M. V. Chekhova, M. Genovese, M. Gramegna, and T. Sh. Iskhakov, "Testing Ultrafast Two-Photon Spectral Amplitudes via Optical Fibres", <i>Optics Express</i> Vol. 18 (2010) 12915.</p> <p>[8] Marina Mondin, Maria Delgado, Fabio Mesiti, Fred Daneshgaran, "Soft-processing for Information Reconciliation in QKD Applications", <i>International Journal of Quantum Information</i>, special issue on "Advances in foundations of Quantum Mechanics and Quantum Information", to appear (2010).</p>
<b>su altre riviste italiane</b>	0	
<b>su altre riviste straniere</b>	0	
<b>comunicazioni a convegni/congressi internazionali</b>	15	<p>[1] F. Vatta, V. Sidorenko, and M. Bossert, "Termination and tailbiting of rate-k/n direct product convolutional codes", <i>Proc. of the 2010 IEEE International Symposium on Information Theory, ISIT'10</i>, Austin, Texas, U.S.A., June 13 - 18, 2010, pp. 2023-2027.</p> <p>[2] Marina Mondin, Fred Daneshgaran, Maria Delgado, and Fabio Mesiti, "Soft-metric-based information reconciliation techniques for QKD", in <i>Proc. SPIE 7815, 781502</i> (2010) doi:10.1117/12.858357, <i>Quantum Communications and Quantum Imaging VIII Conference, Conference Chairs: Ronald E. Meyers, Yanhua Shih, Keith S. Deacon</i>.</p> <p>[3] F. Vatta, A. Schiavi, V. Sidorenko, and M. Bossert, "Termination and tailbiting of direct product convolutional codes", <i>Proc. of the 2009 IEEE Information Theory Workshop, ITW '09</i>, Taormina, Italy, October 11 - 16, 2009, pp. 213-217.</p> <p>[4] Daneshgaran, F.; Laddomada, M.; Mondin, M.; "LDPC-Based Iterative Algorithm for Compression of Correlated Sources at Rates Approaching the Slepian-Wolf Bound", <i>Advances in Satellite and Space Communications</i>, 2009. SPACOMM 2009, First International Conference on, 20-25 July 2009 Page(s):74 - 79.</p> <p>[5] Laddomada, M.; Mesiti, F.; Mondin, M.; "Design of multiplierless decimation filters based on Cyclotomic Polynomials", <i>Circuits and Systems</i>, 2009. MWSCAS '09. 52nd IEEE International Midwest Symposium on, 2-5 Aug. 2009 Page(s):673 - 678.</p> <p>[6] Daneshgaran, F.; Laddomada, M.; Mesiti, F.; Mondin, M.; "On the Throughput Allocation for Proportional Fairness in Multirate IEEE 802.11 DCF", <i>Consumer Communications and Networking Conference</i>, 2009. CCNC 2009. 6th IEEE, 10-13 Jan. 2009 Page(s):1 - 5.</p> <p>[7] A.P. Shurupov, G. Brida, I. Degiovanni, M. Genovese, A. Florio, A. Meda, P. Giorda, and M. Paris, "Optimal evaluation of entanglement in two qubit system", <i>18th International Laser Physics Workshop (LPHYS'09)</i>, July 13 - 17, 2009, Barcelona, Spain</p> <p>[8] Mondin M., F. Daneshgaran, M. Delgado, F. Mesiti, "Novel Techniques for Information Reconciliation, Quantum Channel Probing and Link Design for Quantum Key Distribution", in <i>Proceedings of PSATS 2010</i>, Roma, Italy, February 2010.</p> <p>[9] G. Brida, V. Caricato, M. Genovese, M. Gramegna, M.V. Fedorov., S.P. Kulik, "Entanglement Degree Characterization of Spontaneous Parametric-Down Conversion Biphotons in Frequency Domain", <i>Quantum Communication and Quantum Networking Publisher, Springer, Berlin Heidelberg</i>, pag.46, A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): <i>QuantumCom 2009</i>.</p> <p>[10] G. Brida, M. Genovese, M. Gramegna, F. Piacentini, S. Olivares, and M. G. A. Paris, "On/off Detection Method for Reconstructing the Statistics of Quantum Optical States: An Overview", <i>Proceedings ICQNM 2009 - The Third International Conference on Quantum, Nano and Micro Technologies</i>, 1-7 February 2009 Cancun, Mexico.</p> <p>[11] A. Avella, G. Brida, I. P. Degiovanni, M. Genovese, M. Gramegna, and P. Traina "Experimental quantum cryptography scheme based on orthogonal states: preliminary results" <i>Proc. SPIE Vol. 7702, 77020E</i> (2010).</p> <p>[12] F. Vatta, R. Romano, and F. Mesiti, "Analysis and design of parallel concatenated channel codes for Quantum Key Distribution (QKD) applications", <i>Proc. di ISABEL 2010</i>, Roma, 7-10 Novembre 2010.</p> <p>[13] Stefano Olivares, Matteo G. A. Paris, Maria Delgado and Marina Mondin "Toward a "soft" output quantum channel via Bayesian estimation", <i>Proc. di ISABEL 2010</i>, Roma, 7-10 Novembre 2010.</p> <p>[14] Alessio Avella, Giorgio Brida, Ivo Pietro Degiovanni, Marco Genovese, Marco Gramegna and Paolo Traina, "Experimental realization of Goldenberg - Vaidman QKD Protocol", <i>Proc. di ISABEL 2010</i>, Roma, 7-10 Novembre 2010.</p> <p>[15] Fabio Mesiti, Fred Daneshgaran, Maria Delgado and Marina Mondin, "Sparse-graph codes for information reconciliation in QKD applications invited paper", <i>Proc. di ISABEL 2010</i>, Roma, 7-10 Novembre 2010.</p>
<b>comunicazioni a convegni/congressi nazionali</b>	0	
<b>rapporti interni</b>	0	
<b>brevetti depositati</b>	0	
<b>TOTALE</b>	<b>23</b>	

Per ogni campo di testo max 8.000 caratteri spazi inclusi

Data 21/12/2010 07:04

Firma .....

Si autorizza alla elaborazione e diffusione delle informazioni riguardanti i programmi di ricerca presentati ai sensi del D. Lgs. n. 196/2003 del 30.6.2003 sulla "Tutela dei dati personali". La copia debitamente firmata deve essere depositata presso l'Ufficio competente dell'Ateneo.