Curriculum Vitæ et Studiorum di

Roberto De Prisco

Febbraio 2014

Indice

1 Dati personali

Roberto De Prisco
Dipartimento di Informatica ed Applicazioni
Università degli Studi di Salerno
84084 Fisciano (SA)

Tel./Fax: 089-969722
E-mail: robdep@dia.unisa.it
URL: http://www.dia.unisa.it/~robdep

2 Posizioni

- *2001 - oggi:* Professore associato (gruppo dsciplinare INF/01) presso la Facoltà di Scienze Matematiche Fisiche e Naturali dell'Università degli Studi di Salerno.
- *1998 - 2001:* Ricercatore (gruppo dsciplinare INF/01) presso la Facoltà di Scienze Matematiche Fisiche e Naturali dell'Università degli Studi di Salerno.

3 Titoli di studio

- *2007: Diploma di Pianoforte*, conseguito al Conservatorio di Musica G. Martucci di Salerno.
- *2000: PhD (Doctor of Philosophy)* in "Electrical Engineering and Computer Science", conseguito al Massachusetts Institute of Technology, Cambridge, MA, USA.
- *1998: Dottorato* in "Matematica Applicata ed Informatica", conseguito all'Università degli studi di Napoli.
- *1997: SM (Master of Science)* in "Electrical Engineering and Computer Science", conseguito al Massachusetts Institute of Technology, Cambridge, MA, USA.
- *1991: Laurea* in "Scienze dell'Informazione", conseguita all'Università degli Studi di Salerno.

4 Formazione all'estero

- *Febbraio 2000 - Gennaio 2002*: Visiting Scientist nel gruppo di ricerca Theory of Distributed Systems del Laboratory for Computer Science presso il Massachusetts Institute of Technology.
- *Ottobre 1999 - Gennaio 2002*: Research Scientist presso Akamai Technologies nel gruppo di Distributed Data Collection.

- *Settembre 1995 - Febbraio 2000*: Studente di dottorato (PhD) presso il Laboratory for Computer Science del Massachusetts Institute of Technology.
- *Giugno 1998 - Settembre 1998*: Visiting Scientist presso AT&T Research-Labs, Florham Park, NJ, USA. Collaborazione scientifica con Dr. Dahlia Malkhi e Dr. Michael Reiter.
- *Ottobre 1992 - Ottobre 1993*: Visiting Student presso il Dipartimento di Computer Science della Columbia University, New York, USA. Attività di ricerca svolta in collaborazione con il Dr. Moti Yung.

5 Attività didattica

- Il Prof. De Prisco svolge la sua attività didattica principalmente per il corso di laurea in Informatica (vecchio ordinamento, triennale e specialistica) dell'Università di Salerno.

  Attualmente insegna i seguenti corsi:

  - Programmazione 1 (corso tenuto dall'anno accademico 2013-2014)
  - Musimatica (corso tenuto dall'anno accademico 2006-2007)

  In passato ha insegnato i seguenti corsi:

  - Reti di Calcolatori (dal 2003 al 2014)
  - Sicurezza su Reti (dal 2006 al 2008)
  - Algoritmi e Strutture Dati (dal 2003 al 2005)
  - Algoritmi e Strutture Dati - progetto CAMPUS (dal 2003 al 2005)
  - Algoritmi Distribuiti (2002-2003, per il Dottorato di Ricerca)
  - Algoritmi Distribuiti (2009, scuola di Bertinoro)
  - Laboratorio di Sistemi Operativi (dal 2001 al 2003)

- Ha svolto il ruolo di Teaching Assistant contribuendo con con lezioni settimanali, ricevimento studenti, preparazione e correzione di compiti settimanali e degli esami, per i seguenti corsi:

  - Autunno 1998: *Introduction to Algorithms*, Corso undergraduate tenuto al MIT dai Proff. S. Goldwasser e B. Maggs
  - Autunno 1996: *Introduction to Algorithms*, Corso undergraduate tenuto al MIT dal Prof. C.E. Leiserson

- È stato relatore di numerose tesi di laurea in Scienze dell'Informazione ed Informatica presso l'Università degli Studi di Salerno.
- È membro di commissioni per l'esame di laurea in Scienze dell'Informazione e per l'esame di Diploma in Informatica presso l'Università degli Studi di Salerno.
- Durante il semestre estivo del 1997 è stato tutor per il *Summer Program* organizzato dal *Research Science Institute* presso il MIT, con funzione di supervisore della ricerca svolta.

6 Attività professionali

- Ha svolto il ruolo di Guest Editor per una special issue della rivista Computer Networks (Elsevier) dal titolo "Algorithmic Problems in Distributed Systems", Vol. 50 (10), 14 Luglio 2006.
- Ha svolto (o sta svolgendo) il ruolo di General Chair per le seguenti conferenze internazionali:
  - *Security and Cryptography for Networks 2014* (SCN 2014), 3-5 Settembre 2014, Amalfi, Italia.
  - *Security and Cryptography for Networks 2012* (SCN 2012), 5-7 Settembre 2012, Amalfi, Italia.
  - *Security and Cryptography for Networks 2010* (SCN 2010), 13-15 Settembre 2010, Amalfi, Italia.
  - *Security and Cryptography for Networks 2008* (SCN 2008), 10-12 Settembre 2008, Amalfi, Italia.
  - *Security and Cryptography for Networks 2006* (SCN 2006), 6-8 Settembre 2006, Maiori, Italia.
  - *Distributed Computing 2003* (DISC 2003), 1-3 Ottobre 2003, Sorrento, Italia.
- Ha svolto il ruolo di membro del comitato di programma di varie conferenze internazionali e workshop:
  - SIROCCO 2008, 17-20 Giugno, 2008, Villars-sur-Ollon, Svizzera.
  - WMAN 2005, 5th IEEE International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks, 4-8 Aprile 2005, Denver, Colorado, USA.
  - DSN 2004, Dependable Systems and Networks, 28 Giugno - 1 Lugio 2004, Firenze, Italia.
  - IADIS 2004, International Conference on Applied Computing, 23-26 Marzo 2004, Lisbona, Portogallo.
  - DISC 2003, Distributed Computing, 1-3 Ottobre 2003, Sorrento, Italia.
  - SIROCCO 2000, International Colloquium on Structural Information and Communcatiom Complexity, 20-22 Giugno 2000, L'Aquila, Italia.
  - CS&I 2000, The Fifth International Conference on Computer Science and Informatics, 27 Febbraio - 3 Marzo 2000, Atlantic City, NJ, USA.
- Ha organizzato, nel periodo 1997-1999, il ciclo di seminari del gruppo *Theory of Distributed Systems* del Laboratory for Computer Science, MIT.
- Ha svolto, e svolge regolarmente, revisioni di lavori scientifici sia per riviste che per conferenze.
  - Riviste:
    - Designs, Codes and Cryptography,
    - Distributed Computing,

    - Discrete Applied Mathematics,
    - IEEE Transaction on Software Engineering,
    - IEEE Transaction on Image Processing,
    - IEEE Transaction on Information Theory,
    - IEEE Transaction on Information Forensics and Security,
    - IEEE Transactions on Communications,
    - Information Processing Letters,
    - Information Sciences,
    - International Journal of Distributed Sensor Networks,
    - Theoretical Computer Science,
    - The Computer Journal,
    - Pattern Recignition.
  - Conferenze:
    - PODC (Principle of Distributed Computing),
    - DISC (Distributed Computing),
    - ICALP (International Colloquium on Automata Languages and Programming),
    - SIROCCO (International Colloquium on Structural Information and Communication Complexity).
    - WDAG (Workshop on Distributed Algorithms),
    - DSN (Dependable Systems and Networks),
    - ICTCS (Italian Conference on Theoretical Computer Science),
    - ISAAC (International Symposium on Algorithms and Computation),
    - SRDS (Symposium on Reliable Distributed Systems),

7 Attività di ricerca

Il Prof. De Prisco ha svolto e svolge ricerca su vari temi che possono essere inquadrati in più aree dell'informatica: algoritimi e strutture dati, sistemi distribuiti, reti di calcolatori, crittografia. Un'elenco approssimativo dei vari temi di ricerca è :

- Sistema DNS e traffico Internet
- Algoritmi per agenti egoistici
- Servizi di comunicazione di gruppo
- Problemi di consenso
- Algoritmi e strutture dati
- Crittografia visuale
- Posta elettronica certificata
- Compressione dati

- Musimatica

Nel seguito vengono descritti brevemente i vari temi di ricerca nei quali il Prof. De Prisco è o è stato impegnato:

- *Internet e DNS.* Uno dei principali esempi di sistema distribuito è la rete mondiale nota con il nome di Internet. Tale sistema distribuito è notevolmente complesso e difficile da modellare e studiare. Esso è costituito da migliaia di entità, dette Sistemi Autonomi (AS), ognuna delle quali gestisce un piccolo pezzo del sistema totale. Molti di questi sistemi autonomi sono a loro volta sistemi distribuiti molto complessi. Data l'eterogeneicità dei componenti della rete Internet e il numero elevato di variabili che entrano in gioco nell'analisi del traffico di Internet è difficile fornire dei modelli matematici che permettano di risolvere, da un punto di vista teorico, problemi fondamentali quali, ad esempio, l'istradamento del traffico e la traduzione dei nomi di dominio (sistema DNS). L'assenza di un modello matematico soddisfacente rende importante l'analisi empirica del sistema dalla quale poi si possano trarre delle conlcusioni che permettano di migliorare il sistema. Tuttavia l'enormità del sistema (Internet copre letteralmente tutto il globo) rende difficile qualsiasi analisi empirica globale. In tale ambito il Prof. De Prisco ha studiato il sistema dei nomi di domini sfruttando una analisi empirica fatta su una frazione significativa di Internet. In particolare si è fornito uno studio dell'uso e della disponibilità dei server DNS ([49]). Inoltre è stato studiato il traffico Internet relativo a siti web (protocollo HTTP) a livello di sistemi autonomi ([50]).

- *Algoritmi per Agenti Egoistici.* Per molti problemi reali si può dare un modello matematico in cui i partecipanti al problema sono degli "agenti egoisti" che partecipano alla risoluzione del problema badando solo al proprio personale interesse e non ad un eventuale interesse collettivo. In tali situazioni è molto importante fornire degli algoritmi che permettano di raggiungere l'interesse collettivo. Un esempio pratico ci è dato da Internet: la miriade di componenti di Internet sono possedute da differenti organizzazioni che la utilizzano con differenti finalità. Spesso e volentieri le scelte fatte da ogni singola organizzazione sono mirate a massimizzare un proprio profitto e non, ad esempio, l'efficienza globale dell'intera rete Internet. Le metodologie necessarie per affrontare questo tipo di problemi ci vengono date dalla teoria dei giochi non-cooperativi e dalla microeconomia, dove queste problematiche sono studiate sin dagli anni 50, con i primi studi di Nash. In questi ambiti la progettazione di algoritmi che garantiscono buone prestazioni anche in presenza di agenti egoisti è ottenuta con l'ausilio di un pagamento da offrire agli agenti egoisti per indurli a cooperare. Usando l'algoritmo unitamente ai pagamenti si riescono ad ottenere i risultati voluti. In gergo si utilizza il nome "meccanismo" per indicare una tale soluzione. I classici risultati della teoria dei giochi, se applicati in ambito informatico, devono però essere rivisti alla luce della loro efficienza computazionale. Infatti in molte situazioni fornire un meccanismo richiede la soluzione di problemi computazionalmente difficili. Diventa quindi importante fornire dei meccanismi approssimati. In tale ambito, Il Prof. De Prisco si è occupato del problema dell'assegnazione di attività ad un insieme di macchine con velocità correlate in modo da miniminizzare il tempo massimo di completamento. Alcune varianti del problema sono state considerate: gli agenti egoisti possono avere il controllo delle macchine o dei lavori da assegnare alle macchine; possono mentire senza condizioni; possono mentire ma sono soggetti a verifica alle fine dell'esecuzione ([10,1112,45,52,53]

- *Servizi di comunicazione di gruppo.* L'utilizzo di servizi di comunicazione di gruppo è un approccio di successo nello sviluppo di applicazioni distribuite che tollerano guasti. Tali servizi offrono degli strumenti di comunicazione che facilitano lo sviluppo delle applicazioni. Sebbene vari servizi di comunicazione di gruppo siano usati in sistemi reali, esiste una notevole carenza di specifiche formali di tali servizi. Recentemente, molti sforzi sono stati fatti da ricercatori del settore nel tentativo di sopperire a tale carenza. In tale ambito il Prof. De Prisco ha studiato e proposto vari servizi di comunicazione di gruppo, fornendo specifiche formali del loro comportamento e prove di correttezza. Il modello formale utilizzato è l'IOA (Input-Output Automaton), sviluppato dalla Prof.ssa Lynch presso il MIT. I contributi della ricerca del Prof. De Prisco possono essere riassunti nei seguenti punti: specifiche formali per servizi di comunicazione di gruppo, estensione di tali specifiche a sistemi dinamici e utilizzo del concetto di "quorum" all'interno del servizio di comunicazione; implementazione di tali sistemi usando il linguaggio IOA; sviluppo di applicazioni che utilizzano i servizi di comunicazione di gruppo sopra menzionati; prove formali della correttezza degli algortimi sviluppati. Il Prof. De Prisco ha anche sviluppato un particolare modello di IOA (il Clock General Timed Automaton) utile per trattare sistemi distribuiti asincroni ([58,57,64]).

- *Problemi di consenso.* Il problema del consenso distribuito è l'astrazione di molti problemi di coordinazione presenti nei sistemi distribuiti. Per questo motivo esso è un problema di fondamentale importanza ed è stato molto studiato. Il Prof. De Prisco si è occupato di alcune varianti di tale problema fornendo in alcuni casi prove di impossibilità ed in altri algoritmi ([16,17,56,64]).

  Tra l'altro, usando il modello formale fornito dal Clock General Timed Automaton ha implementato e provato la correttezza di un algoritmo per il consenso distribuito proposto da Leslie Lamport ([18,60]).

- *Algoritmi e strutture dati.* Il Prof. De Prisco ha svolto vari progetti di ricerca nell'area degli algoritmi e strutture dati fra i quali:

  - *Costruzione di alberi binari.* Ha fornito algoritmi per la costruzione di alberi binari (di ricerca e non) che ottimizzano o il costo dell'albero o il tempo di costruzione ([30]).
  - *Efficienza degli alberi binari.* Ha studiato il costo di strutture dati ed algoritmi rappresentati da alberi binari (di ricerca e non) fornendo limitazioni a tale costo per particolari classi di alberi ([25]).
  - *Proprietà combinatoriche di alberi binari.* Ha fornito una generalizzazione della nota disuguaglianza di Kraft-McMillan utilizzando l'altezza "destra" e l'altezza "sinistra" delle foglie, anzichè l'altezza totale, data dalla somma dell'altezza destra e di quella sinistra, considerata nella disuguaglianza di Kraft-McMillan ([28]).
  - *Algoritmi per array lineari di processori.* Ha sviluppato algoritmi per il testing e la riconfigurazione di tali sistemi di computazione ([21,63]).

- *Crittografia Visuale.* La crittografia visuale permette di condividere un'immagine segreta fra un insieme di partecipanti ognuno dei quali riceve informazioni parziali (una *share*) riguardo all'immagine segreta in modo tale che solo determinati sottoinsiemi dei partecipanti (chiamati insiemi qualificati) siano capaci di ricostruire il segreto, mentre tutti gli altri sottoinsiemi (non qualificati) non possono avere alcuna informazione sul

segreto. Una versione più generale di tale problema è il problema della condivisione di segreti (secret sharing). La crittografia visuale può essere vista come un particolare metodo di secret sharing in cui il segreto è un'immagine e le share sono anch'esse delle immagini stampate su delle trasparenze. La peculiarità della crittografia visuale sta nel metodo di ricostruzione del segreto: basta sovrapporre le share (trasparenze). Quindi la computazione necessaria a ricostruire il segreto (che nel secret sharing generale può essere di qualsiasi natura) in questo caso è svolta dal sistema visivo umano. Tale caratterstica rende appetibile l'uso della crittografia visuale in situazioni in cui insiemi qualificati non hanno a disposizione apparecchiature per effettuare la fase di ricostruzione del segreto a partire dalle share. Originariamente la ricerca nell'ambito della crittografia visuale, inventata da Naor e Shamir, ha considerato solo immagini segrete in bianco e nero, cioè costituite da pixel o bianchi o neri. Solo recentemente gli schemi di crittografia visuale sono stati estesi ad immagini colorate. Il Prof. De Prisco si è occupato di problematiche relative a schemi di crittografia visuale in cui l'immagine segreta è composta da pixel colorati fornendo degli schemi che migliorano risultati precedenti. Inoltre il Prof. De Prisco ha proposto un nuovo modello per la crittografia visuale a colori. In tale modello vengono considerate alcune proprietà reali della sovrapposizione di colori che erano state ignorate in ricerche precedenti ([13,14,44,48,55]).

- *Posta elettronica certificata.* Il Prof. De Prisco si è anche occupato di posta elettronica certificata. La posta elettronica sta diventando sempre più utilizzata grazie alla sua praticità d'uso. Essa però non gode di alcune particolari proprietà che sono cruciali in alcuni casi. Ad esempio, non è possibile stabilire con certezza l'identità del mittente; non è possibile avere una ricevuta che certifica la data e l'ora della spedizione; non è possibile essere sicuri che il messaggio sia stato recapitato al destinatario. Tali proprietà sono indispensabili per usi "ufficiali" (quali ad esempio concorsi pubblici). Con l'uso di tecniche crittografiche è possibile ottenere le proprietà richieste; si parla in tal caso di posta elettronica certificata. Il Prof. De Prisco si è occupato del progetto di nuovi protocolli per la posta elettronica certificata ([31]).

- *Compressione dati.* La compressione dati è di fondamentale importanza per le memorizzazione e la trasmissione di dati in quanto permette di ridurre lo spazio necessario alla memorizzazione ed il tempo necessario per la trasmissione. Uno degli algoritmi di compressione più noti ed utilizzati è l'algoritmo di Huffman. Il Prof. De Prisco ha studiato l'efficienza dei codici di Huffman fornendo nuove limitazioni, superiori ed inferiori, alla compressione ottenuta utilizzando i codici di Huffman ([20,23,24,26]).

- *Musimatica.* Recentemente il Prof. De Prisco ha iniziato ad interessarsi dell'applicazione di strumenti informatici alla musica con particolare riferimento alla composizione automatica ([42,41]). Sta sviluppando un software capace di utilizzare le regole classiche dell'armonia per produrre in modo automatico delle composizioni musicali. A tal fine vengono studiate ed utilizzate tecniche spesso utilizzate in intelligenza artificali, quali reti neurali ed algoritmi genetici. Simili linee di ricerca sono seguite da vari altri ricercatori e musicisti, fra i quali si cita David Cope dell'Università della California. Il Prof. De Prisco è responsabile del Laboratorio di Musimatica (computer music) presso il Dipartimento di Informatica dell'Università di Salerno.

8 Attività di consulenza

- Svolge attività di consulenza per l'azienda Akamai Technologies, Cambridge, USA, un'azienda leader nel campo del traffico Internet per siti Web (Web Content Delivery). Durante la collaborazione scientifica del 1999-2002 il Prof. De Prisco ha partecipato al progetto ed allo sviluppo di un sistema di database distribuito capace di gestire un flusso di dati di diversi terabyte giornalieri. Grazie alla conoscenza del sistema acquisita nella fase di progetto e sviluppo è tutt'oggi chiamato a svolgere attività di consulenza per Akamai. Le consulenze svolte hanno portato anche alla stesura di lavori scientifici pubblicati in conferenze che si occupano di problematiche relative ad Internet [49,50].

9 Attività musicali

- È responsabile del laboratorio di Musimatica (computer music) presso il dipartimento di Informatica ed Applicazioni dell'Università di Salerno. Ha conseguito il Diploma di compimento superiore di Pianoforte presso il Conservatorio Statale di Musica "G. Martucci" di Salerno; È membro del direttivo dell'associazione Musicateneo che promuove varie attività musicali all'interno dell'ateneo salernitano. Suona il sassofono contralto con l'Orchestra Jazz dell'Università di Salerno ed è pianista e responsabile del gruppo musicale 30inTango dell'Università di Salerno. L'attività di ricerca in questo campo è indirizzata verso lo studio di tecniche di composizione (musicale) automatica.

10 Elenco delle pubblicazioni

Libri

1. Curatore e traduttore dell'edizione italiana del libro "Data Communications and Networking", B.A. Forouzan, Mac-Graw Hill. Prima edizione italiana, "Reti di Calcolatori e Internet", ISBN 978-88-386-6411, 2007.

Capitoli

2. "Probabilistic Visual Cryptography", Capitolo 6 del libro "Visual Cryptography and Secret Image Sharing". S. Cimato, R. De Prisco, A. De Santis. CRC press, ISBN: 9781439837214, 2012.

3. "Visual Cryptogrpahy for Color Images", Capitolo 12 del libro "Visual Cryptography and Secret Image Sharing". S. Cimato, R. De Prisco, A. De Santis. CRC press, ISBN: 9781439837214, 2012.

Editor

4. Editors: I. Visconti, R. De Prisco,
   Security and Cryptography for Networks (SCN), 6th International Conference, Amalfi, Italy, 5-7 settembre, 2012,
   Vol. 7485, Lecture Notes in Computer Science, Springer-Verlag, 2012

5. Editors: J. Garay, R. De Prisco
   Security and Cryptography for Networks (SCN), 7th International Conference, Amalfi, Italy, 13-15 settembre, 2010,
   Vol. 6280, Lecture Notes in Computer Science, Springer-Verlag, 2010

6. Editors: R. De Prisco, M. Yung,
   Security and Cryptography for Networks (SCN), 5th International Conference, Maiori, Italy, 6-8 settembre, 2006,
   Vol. 4116, Lecture Notes in Computer Science, Springer-Verlag, 2006

7. Guest editors: R. De Prisco, S. Rajsbaum.
   "Algorithmic Problems in Distributed Systems",
   "Special issue" di *Computer Networks* (Elsevier), Vol. 50, No. 10, 2006.

Riviste Internazionali

8. Roberto De Prisco, Alfredo De Santis,
   "On the Relation of Random Grid and Deterministic Visual Cryptography",
   IEEE Transactions on Information Forensics & Security, in pubblicazione.

9. Roberto De Prisco, Alfredo De Santis,
   "Color visual cryptography schemes for black and white secret images",
   Theor. Comput. Sci., 510, pp. 62-86, 2013

10. Roberto De Prisco, Alfredo De Santis,
    "Cheating Immune Threshold Visual Secret Sharing", *Comput. J.*, 53(9), pp. 1485-1496, 2010

11. V. Auletta, R. De Prisco, P. Penna, G. Persiano,
    "The power of verification for one-parameter agents",
    Journal of Computer and System Sciences, Vol. 75 (3), pp. 190-211, 2009.

12. V. Auletta, R. De Prisco, P. Penna, G. Persiano,
    "On designing truthful mechanisms for online scheduling",
    Theoretical Computer Science, Vol 410 (36), pp. 3348-3356, 2009.

13. V. Auletta, R. De Prisco, P. Penna, G. Persiano,
    "Routing selfish unsplittable traffic",
    ACM Transactions on Algorithms, Vol. 3 (4), 2007.

14. S. Cimato, R. De Prisco, A. De Santis,
    "Colored visual cryptography without color darkening",
    Theoretical Computer Science, Vol. 374 (1-3), pp. 261-276, 2007.

15. S. Cimato, R. De Prisco, A. De Santis,
    "Probabilistic Visual Cryptography",
    The Computer Journal, Vol. 49 (1), pp.97-107, 2006.

16. S. Cimato, R. De Prisco, A. De Santis,
    "Optimal Colored Threshold Visual Cryptography Schemes",
    Designs, Codes and Cryptography, Vol. 35 (3), pp. 311-335, 2005.

17. R. De Prisco, D. Malkhi e M. Reiter,
"On k-set consensus problems in asynchronous systems".
IEEE Transactions on Parallel and Distributed Systems,
Vol. 12 (1), pp. 7-21, 2001.

18. B. Chlebus, R. De Prisco e A. Shvartsman,
"Performing tasks on restartable message-passing processors".
Distributed Computing, Vol. 14 (1), pp. 49-64, 2001.

19. R. De Prisco, B. Lampson e N. Lynch,
"Revisiting the Paxos algorithm",
Theoretical Computer Science, Vol. 243, pp. 35-91, 2000

20. R. De Prisco e A. De Santis,
"On lower bounds for the redundancy of optimal codes",
Design, Codes and Cryptography, Vol. 15, pp. 29-45, 1998.

21. R. De Prisco e A. De Santis,
"On the data expansion of the Huffman compression algorithm",
The Computer Journal, Vol. 41 (3), pp. 137-144, 1998.

22. R. De Prisco, A. Monti e L. Pagli,
"Testing and reconfiguration of VLSI linear arrays",
Theoretical Computer Science, Vol. 147 (1-2), pp. 171-188, 1998.

23. R. De Prisco e A. De Santis,
"Catastrophic faults in reconfigurable linear arrays of processors",
Discrete Applied Mathematics, Vol. 75 (2), pp. 105–123, 1997.

24. R. De Prisco e A. De Santis,
"A new bound for the data expansion of Huffman codes",
IEEE Trans. on Information Theory, Vol. 43 (6), pp. 2028–2032, 1997.

25. R. De Prisco e A. De Santis,
"New lower bounds on the cost of binary search trees",
Theoretical Computer Sciences, Vol. 156 (1-2), pp. 315–325, 1996.

26. R. De Prisco, G. Parlati e G. Persiano,
"A note on the expected path length of trees with known fringe",
Information Processing Letters, Vol. 59 (6), pp. 309–315, 1996.

27. R. De Prisco e A. De Santis,
"On the redundancy achieved by Huffman codes",
Information Sciences, Vol. 88 (1-4), pp. 131–148, 1996.

28. C. Blundo e R. De Prisco,
"New bounds on the expected length of one-to-one codes",
IEEE Trans. on Information Theory, Vol. 42 (1), pp. 246–249, 1996.

29. R. De Prisco e G. Persiano,
"Characteristic inequalities for binary trees",
Information Processing Letters, Vol. 53 (4), pp. 201–207, 1995.

30. R. De Prisco, G. Parlati e G. Persiano,
"Minimal path length of trees with known fringe",
Theoretical Computer Science, Vol. 143 (1), pp. 175–188, 1995.

31. R. De Prisco e A. De Santis,
"On binary search trees",
Information Processing Letters, Vol. 45, pp. 249–253, 1993.

Riviste Internazionali in formato elettronico

32. C. Blundo, S. Cimato, R. De Prisco, A. L. Ferrara,
"Modeling A Certified Email Protocol using I/O Automata",
Electr. Notes Theor. Comput. Sci., Vol. 99, pp. 339-359, 2004.

Conferenze Internazionali

33. Paolo D'Arco, Roberto De Prisco,
"Secure Two-Party Computation: A Visual Way",
Proceedings of ICITS 2013, pp. 18-38, LNCS 8317, 2014.

34. Paolo D'Arco, Roberto De Prisco, Alfredo De Santis
"Measure-Independent Characterization of Contrast Optimal Visual Cryptography Schemes",
Proceedings of ICITS 2013, pp. 19-55, LNCS 8317, 2014.

35. A. Castiglione, G. Cattaneo, R. De Prisco, A. De Santis, K. Yim,
"How to Forge a Digital Alibi on Mac OS X" Proceedings of CD-ARES 2012, pp. 430-444, 2012.

36. A. Capozzi, R. De Prisco, M. Nasti, R. Zaccagnino,
"Musica Parlata: a methodology to teach music to blind people", Proceedings of ASSETS 2012, pp. 245-246, 2012.

37. R. De Prisco, G. Zaccagnino, R. Zaccagnino,
"A Differential Evolution Algorithm Assisted by ANFIS for Music Fingering", Proceedings of ICAISC, Springer LNCS 7269, pp. 48-56, 2012.

38. R. De Prisco, G. Zaccagnino, R. Zaccagnino,
"A Genetic Algorithm for Dodecaphonic Compositions", Proceedings of EvoApplications, Springer LNCS 6625 (Part II), pp. 244-253, 2011.

39. R. De Prisco, P. Sabatino, G. Zaccagnino, R. Zaccagnino,
"A Customizable Recognizer for Orchestral Conducting Gestures Based on Neural Networks", Proceedings of EvoApplications, Springer LNCS 6625 (Part II), pp. 254-263, 2011.

40. G, Acampora, J. M. Cadenas, R. De Prisco, V. Loia, E. M. Ballester, R. Zaccagnino,
"A hybrid computational intelligence approach for automatic music composition", Proceedings of FUZZ-IEEE, pp. 202-209, 2011.

41. R. De Prisco, A. De Santis,
"Using Colors to Improve Visual Cryptography for Black and White Images", Proceedgins of ICITS 2011, LNCS 6673, pp. 182-201, 2011.

42. R. De Prisco, A. Eletto, A. Torre, R. Zaccagnino,
"A Neural Network for Bass Functional Harmonization",
EvoWorkshops 2010, Istanbul, Turkey. Apparirà nella serie Lecture Notes in Computer Science, Springer, 2010.

43. R. De Prisco, R. Zaccagnino,
"An Evolutionary Music Composer Algorithm for Bass Harmonization",
EvoWorkshops 2009, Tbingen, Germany. Vol. 5484, Lecture Notes in Computer Science, Springer, pp. 567-572, 2009.

44. A. Castiglione, R. De Prisco, A. De Santis,
"Do You Trust Your Phone?",
EC-Web 2009, Linz, Austria. Lecture Notes in Computer Science, Vol. 5692, Springer, pp. 50-61, 2009.

45. R. De Prisco, A. De Santis,
"Cheating Immune (2,)-Threshold Visual Secret Sharing",
SCN 2006, Vol. 4116, Lecture Notes in Computer Science, Springer, pp.216-228, 2006

46. V. Auletta, R. De Prisco, P. Penna, G. Persiano, C. Ventre,
"New Constructions of Mechanisms with Verification",
ICALP 2006, Vol. 4051, Lecture Notes in Computer Science, Springer, pp.596-607, 2006

47. C. Blundo, S. Cimato, R. De Prisco,
"A Lightweight Approach to Authenticated Web Caching",
negli atti del convegno IEEE/IPSJ International Symposium on Applications and the Internet (SAINT 2005), Trento, Italy, 2005. IEEE Computer Society 2005, ISBN 0-7695-2262-9, pp. 157–163.

48. V. Auletta, R. De Prisco, P. Penna, G. Persiano,
"On Designing Truthful Mechanisms for Online Scheduling",
negli atti del 12^o convegno internazionale SIROCCO 2005, Mont Saint-Michel, France, 2005. LNCS 3499, Springer, pp 3–17, 2005.

49. S. Cimato, R. De Prisco, A. De Santis,
"Colored Visual Cryptography without Color Darkening",
negli atti del 4^o convegno Security in Communication Networks (SCN 04), Amalfi, Italia, 2004.
Springer-Verlag, LNCS 3352, pp. 235-248, 2005.

50. J. Pang, J. Hendricks, A. Akella, R. De Prisco, B. Maggs, S. Seshan,
"Availability, Usage, and Deployment Characteristics of the Domain Name System",
negli atti del 4^o convegno ACM SIGCOMM Internet Measurement Conference (IMC04), pp. 1-14, Taormina, Italia, 2004

51. A. Feldmann, N. Kammenhuber, O. Maennel, B. Maggs, R. De Prisco, R. Sundaram,
"A Methodology for Estimating Interdomain Web Traffic demand",
negli atti del 4^o convegno ACM SIGCOMM Internet Measurement Conference (IMC04) pp. 322-335, Taormina, Italia, 2004

52. V. Auletta, R. De Prisco, P. Penna, G. Persiano,
"The Power of Verification for One-Parameter Agents",
ICALP 2004, Vol. 3142, Lecture Notes in Computer Science, Springer, pp.171-182, Turku, Finlandia, 2004.

53. V. Auletta, R. De Prisco, P. Penna, G. Persiano,
"Deterministic Truthful Mechanisms for Scheduling on Selfish Machines",
STACS 2004, Vol. 2996, Lecture Notes in Computer Science, Springer, pp.608-619, Montpellier, Francia, 2004.

54. V. Auletta, R. De Prisco, P. Penna, G. Persiano,
"How to Route and Tax Selfish Unsplittable Traffic",
negli atti del 16^o convegno ACM Symposium on Parallelism in Algorithms and Architectures (SPAA 2004). Barcellona, Spagna, 2004.

55. C. Blundo, S. Cimato, R. De Prisco,
"Certified Email: Design and Implementation of a New Optimistic Protocol",
negli atti del convegno Symposium on Computers and Communications
IEEE (ISCC 03), pp 828-833, Antalya, Turchia, 2003.

56. S. Cimato, R. De Prisco, A. De Santis,
"Optimal Colored Threshold Visual Cryptography Schemes",
negli atti del convegno International Theory Workshop (ITW 03), Parigi, Francia, 2003.

57. R. De Prisco, D. Malkhi e M. Reiter,
"On k-set consensus problems in asynchronous systems",
atti del 18^o *ACM Symposium on Principles of Distributed Computing (PODC 99)*, Atlanta, Georgia, pp. 257–265, 1999.

58. R. De Prisco, A. Fekete, N. Lynch e A. Shvartsman,
"A dynamic primary configuration group communication service",
atti del 13^o *International Symposium on Distributed Computing (DISC 99)*, Bratislava, Slovak Republic, pp. 64–78, 1999.

59. R. De Prisco, A. Fekete, N. Lynch e A. Shvartsman,
"A dynamic view-oriented group communication service",
atti del 17^o *ACM Symposium on Principles of Distributed Computing (PODC 98)*, Puerto Vallarta, Mexico, pp. 227–236, 1998.

60. R. De Prisco e A. De Santis,
On the redundancy and data expansion of Huffman codes",
atti dell'*International Symposium on Information Theory (ISIT 98)*, Cambridge, MA, pag. 272, 1998.

61. R. De Prisco, B. Lampson e N. Lynch,
"Revisiting the Paxos algorithm",
atti dell'11^o *International Workshop on Distributed Algorithms (WDAG 97)*, Saarbrüken, Germany, Lecture Notes in Computer Science, Vol. 1320, pp. 111–125, 1997.

62. B. Chlebus, R. De Prisco e A. Shvartsman,
"Performing tasks on restartable message-passing processors",

atti dell'11^o *International Workshop on Distributed Algorithms (WDAG 97)*, Saarbrüken, Germany, Lecture Notes in Computer Science, Vol. 1320, pp. 96–110, 1997.

63. R. De Prisco, A. Mayer e M. Yung,
"Time-Optimal Message-Efficient Work Performance in the Presence of Faults",
atti del 13^o *ACM Symposium on Principles of Distributed Computing (PODC 94)*,
Los Angeles, California, USA, pp. 161–172, 1994.

64. R. De Prisco e A. Monti,
"On reconfigurability of VLSI linear arrays",
atti del 3^o *Workshop on Algorithms and Data Structures (WADS 93)*, Montreal, Canada, pp. 553–564, 1993.

Tesi di dottorato

65. R. De Prisco
"On building blocks for distributed systems",
Tesi di PhD, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Techonology, 2000.

66. R. De Prisco
"Sull'efficienza dei codici di Huffman",
Tesi di Dottorato in Matematica applicata ed Informatica, Università di Napoli, 1998.

Tesi di Master

67. R. De Prisco
"Revisiting the Paxos algorithm",
Tesi di Master, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Techonology, 1997.