

CURRICULUM DELL'ATTIVITÀ SCIENTIFICA E DIDATTICA

Ivan Visconti

Attività principali:

Comitati di programma:

1. **Program Chair** di “The 8th Conference on Security and Cryptography for Networks (SCN 2012)” - Amalfi, Italia - *LNCS Springer-Verlag (TBC)*.
2. PC member di “The 31st Advances in Cryptology (EUROCRYPT 2012)” - Cambridge, United Kingdom - **IACR** - *LNCS Springer-Verlag*.
3. PC member di “The 15th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2012)” - Darmstadt, GERMANY - **IACR** - *LNCS Springer-Verlag*.
4. PC member di “The 14th Information Security Conference (ISC 2011)” - Xi'an, China. - *LNCS Springer-Verlag*.
5. PC member di “The 10th International Conference on CRYPTOLOGY AND NETWORK SECURITY (CANS 2011)” - Sanya, China. - *LNCS Springer-Verlag*.
6. PC member di “The 9th International Conference on Applied Cryptography and Network Security (ACNS 2011)” - Malaga, Spain. - *LNCS Springer-Verlag*.
7. PC member di “The 4th International Conference on Cryptology AFRICACRYPT 2011”, Dakar, Senegal. - *LNCS Springer-Verlag*.
8. PC member di “The 9th International Conference on CRYPTOLOGY AND NETWORK SECURITY (CANS 2010)” - Kuala Lumpur, Malaysia. - *LNCS Springer-Verlag*.
9. PC member di “The 13th Information Security Conference (ISC 2010)” - Boca Raton, FL, USA - *LNCS Springer-Verlag*.
10. PC member di “The 7th Conference on Security and Cryptography for Networks (SCN 2010)” - Amalfi, Italia - *LNCS Springer-Verlag*.
11. PC member di “The 13th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2010)” - Parigi, Francia - **IACR** - *LNCS Springer-Verlag*.
12. PC member di “The 8th International Conference on CRYPTOLOGY AND NETWORK SECURITY (CANS 2009)” - Kanazawa, Ishikawa, Japan - *LNCS Springer-Verlag*.

13. PC member di “The 15th Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2009)” - Tokio, Japan - **IACR** - *LNCS Springer-Verlag*.
14. PC member di “The 12th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2009)” - Irvine (CAL), USA - **IACR** - *LNCS Springer-Verlag*.
15. PC member di “The 6th Conference on Security and Cryptography for Networks (SCN 2008)” - Amalfi, Italia - *LNCS Springer-Verlag*.
16. PC member di “RSA Conference 2006, Cryptographers’ Track (RSA 2006)” - San Jose, USA - *LNCS Springer-Verlag*.
17. PC member di “The 2nd Conference on Information Security and Cryptology (IN-SCRYPT 2006)” - Pechino, Cina, *LNCS Springer-Verlag*.
18. PC member di “The 1st Conference on Trust and Privacy in Digital Business (TrustBus 2004)” - Saragozza (Spagna) - *LNCS Springer-Verlag*.

Direzione di sessioni:

1. Session Chair della sessione “Cryptographic Protocols I” per la conferenza “The 7th Conference on Security and Cryptography for Networks (SCN 2010)”, Amalfi (Italia) - *LNCS Springer-Verlag*.
2. Session Chair della sessione “Protocols I” per la conferenza “The 13th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2010)” - Parigi (Francia)- **IACR** - *LNCS Springer-Verlag*.
3. Session Chair della sessione “Models and Frameworks I” per la conferenza “The 15th Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2009)” - Tokio, Japan - **IACR** - *LNCS Springer-Verlag*.
4. Session Chair della sessione “Applications and Protocols” per la conferenza “The 12th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2009)” - Irvine (CAL), USA - **IACR** - *LNCS Springer-Verlag*.
5. Session Chair della sessione “Encryption 3” per la conferenza “The 6th Conference on Security and Cryptography for Networks (SCN 2008)”, Amalfi (Italia) - *LNCS Springer-Verlag*.
6. Session Chair della sessione “Encryption 2” per la conferenza “The 6th Conference on Security and Cryptography for Networks (SCN 2008)”, Amalfi (Italia) - *LNCS Springer-Verlag*.
7. Session chair per “Secure Computation” in “The 35th International Colloquium on Automata, Languages and Programming (ICALP 2008)”, Reykjavik (Islanda) - **EATCS** - *LNCS Springer-Verlag*.
8. Session chair per “Protocols” per il “Workshop on Secure Component and System Identification (SECSI 2008)”, Berlino (Germania).
9. Session chair per “Mobile and Network Security (2)” in “The 8th Australasian Conference on Information Security and Privacy (ACISP 2003)”, Wollongong (Australia) - *LNCS Springer-Verlag*.

Presentazioni su invito:

1. STAR (Seminar on Theory, Algorithms and eRyptography Research) seminar at UCSD (Novembre 2009, La Jolla - CAL - USA).
2. Distinguished Lecturer Seminar Series at UCI (Novembre 2009, Irvine - CAL - USA).
3. Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference II (Giugno 2009, Lake Arrowhead - CAL - USA).
4. Workshop on Cryptographic Protocols and Public-Key Cryptography (Maggio 2009, Bertinoro, Italia).
5. Microsoft Research Colloquium (Novembre 2008, Redmond, USA).
6. Security Hardware in Theory and Practice (Giugno 2008, Dagstuhl, Germania).
7. Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference I (Giugno 2008, Lake Arrowhead - CAL - USA).
8. Workshop on Cryptographic Protocols (Marzo 2007, Bertinoro - Italia).
9. Workshop on Foundations of Secure Multi-Party Computation and Zero-Knowledge (Nov. 2006, Los Angeles - USA).

Principali pubblicazioni:

1. *IACR*: CRYPTO (2004, 2005, 2008, 2009), ASIACRYPT (2004), TCC (2006, 2009, 2010), PKC (2008, 2010).
2. *ACM*: CCS (2000), TISSEC (2003).
3. *EATCS*: ICALP (2005 - 3 papers, 2006, 2008), TCS (2007).
4. *Altre*: CT-RSA (2011), ACNS (2010), ESORICS (2008), Financial Cryptography (2004), Proceedings di SCN (2008).

Principali partecipazioni a progetti di ricerca nazionali/internazionali:

1. **NoE EU**: ECRYPT 2004-2008, ECRYPTII 2008-2012.
2. **STREP EU**: FRONTS 2007-2011.
3. **IP EU**: AEOLUS 2006-2009.
4. **PRIN IT**: 2010-2012.
5. **VIGONI IT-D**: 2009-2010.

Principali attività organizzative:

1. Organizzatore del “Workshop on Protocols and Public-Key Cryptography (2009)” - Bertinoro, Italia, Maggio 2009.
2. General Co-Chair di “The 6th Conference on Security and Cryptography for Networks (SCN 2008)” - Amalfi, Italia, Settembre 2008 - LNCS Springer-Verlag.
3. Organizzatore della “ECRYPT International PhD School on Zero Knowledge: Foundations and Applications (2006)” - Bertinoro, Italia, Novembre 2006.
4. Organizzatore di 2 meeting internazionali relativi al Network of Excellence ECRYPT.

Principali attività didattiche:

1. Ciclo di seminari su “Identification Protocol” per la ECRYPT PhD Summer School on Applied Cryptographic Protocols, Mykonos (Grecia), Settembre 2010.
2. Ciclo di seminari su “Secure Cryptographic Protocols Against Man-in-the-Middle Attacks” per i PhD student in computer science di UCLA, Los Angeles, USA, Novembre/Dicembre 2009.
3. Tutoraggio per l'attività di dottorato di ricerca in Informatica per Alessandra Scafuro (2009-2012).
4. anno accademico 2009/2010 Corso di Recupero di Lab. di Sistemi Operativi (laurea triennale in informatica, Università di Salerno).
5. anni accademici 2005/2006 - 2006/2007 - 2007/2008 - 2008/2009: Lab. di Sistemi Operativi (laurea triennale in informatica, Università di Salerno).
6. anno accademico 2006/2007: Lab. di Crittografia e Sicurezza dell'Informazione (laurea specialistica in informatica, Università di Salerno).
7. anni accademici 2007/2008 - 2008/2009: Strumenti di Crittografia per la Sicurezza dell'Informazione (laurea specialistica in informatica, Università di Salerno).
8. anni accademici 2007/2008: Sicurezza su Reti (laurea triennale in informatica, Università di Salerno).
9. 2005/2008: Relatore di 15 tesi per la laurea triennale in informatica, di 1 tesi per la laurea in informatica (vecchio ordinamento), di 4 tesi per la laurea specialistica in informatica ed attività di tutor per 15 tirocini, all'Università di Salerno.
10. 1998-2003: Vari corsi IFTS, aziendali e master.

Indice

1	Dati Personali	5
2	Principali Interessi di Ricerca	5
3	Conoscenze Avanzate	7
4	Presentazioni di Risultati Scientifici	7
5	Attività Organizzative	11
6	Direzione/Partecipazione di/in Gruppi di Ricerca e Grant	11
7	Presentazioni su Invito	12
8	Comitati di Programma	13
9	Direzioni di Sessioni	14
10	Studi ed Incarichi Ricoperti	15
11	Collaborazioni con Studenti/Dottorandi	17
12	Altre Attività Scientifiche	18
13	Attività Applicative - Convenzioni di Dipartimento	19
14	Partecipazione a Workshop/Conferenze e Meeting	20
15	Articoli Scientifici	26
15.1	Volumi	26
15.2	Riviste	26
15.3	Atti di Convegni	27
15.4	Capitoli di Libri	33
16	Attività Didattiche e Partecipazione a Scuole di Dottorato	33
16.1	Docenze per Studenti di Dottorato	33
16.2	Docenze per Studenti della Laurea	34
16.3	Tesi ed Altre Attività Didattiche	36
16.4	Partecipazione a Corsi e Scuole	37

1 Dati Personali

Nome: Ivan

Cognome: Visconti

Data di nascita: 18 ottobre 1974

Luogo di nascita: Salerno (Italia)

Cittadinanza: Italiana

Residenza: via Gelso n. 93 - 84126 Salerno (SA), Italia

E-mail: visconti@dia.unisa.it

URL: <http://www.dia.unisa.it/~visconti>

2 Principali Interessi di Ricerca

Crittografia basata su complessità computazionale [4, 15, 21, 23, 33]. Partendo dall'assunzione che è facile generare problemi difficili, è possibile costruire fondamentali primitive di crittografia la cui sicurezza viene provata usando il meccanismo delle riduzioni. La ricerca in questo ambito riguarda l'overlapping tra crittografia e teoria della complessità computazionale e mira ad ottenere costruzioni di primitive crittografiche basandole su assunzioni di complessità computazionale congetturate essere vere. Di primaria importanza risultano poi anche ulteriori proprietà quali l'efficienza computazionale, la comunicazione richiesta e le assunzioni fisiche aggiuntive.

Tecnologie per la tutela della privacy [2, 5, 7, 8, 10, 22]. L'uso pervasivo di tecnologie che gestiscono le nostre informazioni espone la privacy degli utenti a numerosi rischi. La ricerca continua di strumenti digitali che offrono servizi più convenienti dei corrispondenti servizi fisici ha indubbiamente trascurato problematiche di riservatezza dei dati il cui uso fraudolento comporta potenziali danni che non tutti sono disposti ad accettare. Tutto questo non può essere gestito unicamente affidandosi alle misure punitive previste dalle normative.

La ricerca in questa area ha lo scopo di analizzare e costruire sistemi che preservino i vantaggi del mondo digitale ma al tempo stesso garantiscono la riservatezza dei dati tutelando quindi la privacy degli utenti. Strumenti fondamentali per tale ricerca sono speciali primitive crittografiche e l'utilizzo di hardware con proprietà di sicurezza. I concetti di anonimizzazione e credenziali digitali sono ulteriori ingredienti a disposizione di chi intende produrre soluzioni soddisfacenti.

Sicurezza delle reti e dei sistemi [3, 6, 9, 12, 18]. Il danno quotidianamente prodotto da attacchi a reti di calcolatori e server è in crescita e raggiunge progressivamente livelli sempre più preoccupanti. La protezione delle reti e dei sistemi contro tali attacchi ha visto nel tempo l'impiego di tecniche sempre più sofisticate, a volte prese in prestito da altri campi come psicologia ed economia.

Uno dei principali obiettivi della ricerca in questo settore riguarda la necessità di trovare soluzioni a misura d'uomo, ossia di sviluppare meccanismi che godono delle proprietà di sicurezza richieste, ma che al tempo stesso possono essere impiegati dagli utenti standard in quanto è di

questo tipo di profilo che si compone la grande maggioranza della popolazione che oggi usa il cyberspace.

Crittografia razionale [27, 34]. Tradizionalmente, la crittografia si occupa di garantire che le parti coinvolte effettuino delle computazioni ottenendo l'output corretto in relazione all'input fornito. La teoria dei giochi invece si occupa dei comportamenti che le parti possono avere e quindi degli input che forniscono, solitamente seguendo un comportamento razionale, con lo scopo di ottenere un'utilità.

Rational cryptography è un'area emergente di ricerca in cui crittografia e teoria dei giochi vengono combinate per fornire protocolli più robusti dove non solo vengono garantite proprietà di privacy e sicurezza, ma vengono anche indotte le parti razionali ad usare gli input corretti.

Rfid e passaporti elettronici [25, 28, 29]. Il tradizionale modello di calcolo distribuito che prevede reti di computer viene progressivamente affiancato da sensori con limitate capacità computazionali, di memoria, comunicazione ed autonomia che tuttavia sono disseminati sul territorio per svolgere diverse funzionalità, tra cui la tracciabilità di merci e persone. Esempi di tali sensori sono i chip RFID che sono attualmente presenti nei passaporti elettronici.

La ricerca in questo settore riguarda lo studio, analisi e progettazione di protocolli ad-hoc per chip con tali limitazioni con l'obiettivo di preservare alcune funzionalità di sicurezza quali la non-trasferibilità delle prove, l'impossibilità di produrre dei cloni o l'abuso nel tracciamento di merci e persone.

Database sicuri [19]. L'uso crescente di informazioni multimediali quali immagini e video e la loro presenza nei database comporta un sempre crescente outsourcing dei dati, ossia di un fenomeno in base al quale il proprietario delle informazioni chiede ad un'altra entità la memorizzazione delle stesse, a causa della loro eccessiva dimensione. Ovviamente l'accesso fraudolento ai dati e la loro manomissione sono obiettivi primari da perseguire quando si effettuano tali transazioni.

La ricerca in questo settore riguarda lo studio di sistemi che permettono di garantire la confidenzialità e consistenza dei dati di un database in outsourcing ed al tempo stesso di poterli esportare. A supporto di tali tecniche esistono recenti strumenti crittografici quali "searchable encryption" e "zero-knowledge sets" che consentono di ottenere interessanti proprietà di privacy e sicurezza ed al tempo stesso di mantenere adeguati livelli di praticità ed utilizzabilità dei servizi.

Protocolli sicuri su reti asincrone [11, 13, 14, 16, 17, 20, 26, 32]. Il tradizionale modello con cui veniva originariamente provata la sicurezza di un protocollo si è dimostrato inadeguato con la diffusione di reti asincrone come Internet. Infatti, un avversario su Internet è in grado di eseguire differenti protocolli concorrentemente, spesso controllando lo scheduling dei messaggi.

La comunità che si occupa della "provable security" ossia della definizione e dell'utilizzo di strumenti la cui sicurezza viene provata secondo un ben definito formalismo, sta quindi recentemente considerando altri paradigmi dove la sicurezza di un protocollo considera anche la sua potenziale esecuzione in concorrenza con altre istanze dello stesso protocollo o di altri protocolli.

Schemi di cifratura con proprietà speciali [24]. Gli schemi di cifratura possono godere di diverse proprietà di sicurezza la cui importanza varia in base all'uso dello schema. In particolare, quando uno schema di cifratura viene utilizzato come sottoprotocollo, le addizionali proprietà possono avere un ruolo chiave per la sicurezza del protocollo esterno.

La ricerca in tal senso considera alcune proprietà speciali come la non-malleabilità completa che ha applicazioni per la progettazione di aste digitali sicure, e “searchable encryption”, che ha applicazioni per la ricerca in dati gestiti in outsourcing.

3 Conoscenze Avanzate

- Sistemi operativi: Unix, Linux, Windows.
- Linguaggi di programmazione: C, C++, Java, Php, Python e altri.
- Protocolli/Architetture: TCP/IP, TLS/SSL, IPSEC, VPN, HTTP, CGI, PKI, X509 e altri.
- Applicativi: OpenSSL, PGP, Apache, MySQL e altri.

4 Presentazioni di Risultati Scientifici

Sono stato speaker per le seguenti presentazioni:

- Febbraio 2010: Efficiency Preserving Transformations for Concurrent Non-malleable Zero Knowledge
Ambito: Conferenza TCC '10
Luogo: Zurigo - Svizzera
- Novembre 2009: Efficiency Preserving Transformations for Concurrent Non-Malleable Zero-Knowledge
Ambito: STAR (Seminar on Theory, Algorithms and cRyptography Research) seminar at UCSD
Luogo: La Jolla (CAL) - USA
- Novembre 2009: Revisiting RFID Security and Privacy
Ambito: Distinguished Lecturer Seminar Series at UCI
Luogo: Irvine (CAL) - USA
- Giugno 2009: Collusion-Free Multi-Party Computation in the Mediated Model
Ambito: Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference II, 2009
Luogo: Lake Arrowhead (CAL) - USA
- Maggio 2009: Collusion-Free Multi-Party Computation in the Mediated Model
Ambito: Conferenza WPK '09
Luogo: Bertinoro, Forlì

- Marzo 2009: Simulation-Based Concurrent Non-Malleable Commitments and Decommitments
Ambito: Conferenza TCC '09
Luogo: San Francisco - USA
- Novembre 2008: Simulation-Based Concurrent Non-Malleable Commitments and Decommitments
Ambito: Microsoft Research Colloquium '08
Luogo: Redmond - USA
- Ottobre 2008: Improved Security Notions and Protocols for Non-Transferable Identification
Ambito: Conferenza ESORICS '08
Luogo: Malaga - Spagna
- Luglio 2008: Constant-Round Concurrent Non-Malleable Zero Knowledge in the Bare Public-Key Model
Ambito: Conferenza ICALP '08
Luogo: Reykjavik - Islanda
- Luglio 2008: Bounded Ciphertext-Policy Attribute-Based Encryption
Ambito: Conferenza ICALP '08
Luogo: Reykjavik - Islanda
- Giugno 2008: Co-soundness in Public-Key Models
Ambito: Provilab (ECRYPT) Meeting
Luogo: Berlino, Germania
- Giugno 2008: Identification Protocols Revisited with RFID Chips and Pufs
Ambito: Security Hardware in Theory and Practice A Marriage of Convenience, 2008
Luogo: Dagstuhl, Germania
- Giugno 2008: Concurrent Non-Malleable Commitments and Decommitments
Ambito: Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference I, 2008
Luogo: Lake Arrowhead (CAL), USA
- Maggio 2008: Identification Protocols Revisited - Episode I: E-Passports
Ambito: AEOLUS Meeting
Luogo: Salerno, Italia
- Marzo 2008: Completely Non-Malleable Encryption Revisited
Ambito: Conferenza PKC '08
Luogo: Barcellona, Spagna
- Marzo 2008: Identification Protocols Revisited - Episode I: E-Passports
Ambito: Conferenza SECSI '08
Luogo: Berlino, Germania

- Febbraio 2008: Co-Sound ZK Proofs with Public Keys
Ambito: Visita nell'ambito del progetto ECRYPT
Luogo: Ruhr-University Bochum, Germania.
- Ottobre 2007: On Defining Proofs of Knowledge in the Bare Public-Key Model
Ambito: Conferenza ICTCS '07
Luogo: Roma, Italia
- Ottobre 2007: Proofs of Knowledge vs Proof Systems
Ambito: Provilab (ECRYPT) Meeting
Luogo: Salerno, Italia
- Giugno 2007: PassePartout Certificates.
Ambito: Workshop PRISE '07
Luogo: Roma, Italia
- Marzo 2007: Concurrent Non-Malleable Commitments Revisited
Ambito: Provilab (ECRYPT) Meeting
Luogo: Louvain-la-Neuve, Belgio
- Marzo 2007: Secure Proof Systems Under Man-in-the-Middle Attacks
Ambito: Conferenza WCP '07
Luogo: Bertinoro, Forlì
- Novembre 2006: Concurrent Non-Malleable Witness Indistinguishability
Ambito: Foundations of secure multi-party computation and zero-knowledge and its applications
Luogo: UCLA, Los Angeles, USA
- Ottobre 2006: Witness Indistinguishability and Its Applications
Ambito: Provilab (ECRYPT) Meeting on Anonymous Credentials
Luogo: Bochum, Germania
- Agosto 2006: On Non-Interactive Zero-Knowledge Proofs of Knowledge in the Shared Random String Model
Ambito: Conferenza MFCS '06
Luogo: Stará Lesná, Slovacchia
- Luglio 2006: Efficient Zero Knowledge on the Internet
Ambito: Conferenza ICALP '06
Luogo: Venezia, Italia
- Marzo 2006: Mercurial Commitments: Minimal Assumptions and Efficient Constructions
Ambito: Conferenza TCC '06
Luogo: New York, USA

- Settembre 2005: Zero-Knowledge Databases
Ambito: Provilab (ECRYPT) Meeting on Secure and Practical Protocols
Luogo: Roma, Italia
- Luglio 2005: Concurrent Zero Knowledge in the Public-Key Model
Ambito: Conferenza ICALP '05
Luogo: Lisbona, Portogallo
- Aprile 2005: Self-Concurrent Composition of Two-Party Protocols
Ambito: Provilab (ECRYPT) Meeting on Protocol Composition
Luogo: Zurigo, Svizzera
- Dicembre 2004: Improved Setup Assumptions for 3-Round Resettable Zero Knowledge
Ambito: Conferenza ASIACRYPT '04
Luogo: Jeju, Corea
- Agosto 2004: Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model
Ambito: Conferenza CRYPTO '04
Luogo: Santa Barbara, California, USA
- Aprile 2004: Efficient and Non-malleable Proofs of Plaintext Knowledge and Applications (seminario)
Ambito: Gruppo di lavoro dell'ENS
Luogo: ENS, Parigi, Francia
- Febbraio 2004: An Efficient and Usable Multi-Show Non-Transferable Anonymous Credential System
Ambito: Conferenza FC '04
Luogo: Key West, Florida, USA
- Novembre 2003: Resettable Zero Knowledge with Public Keys (seminario)
Ambito: Seminario settimanale dell'ENS
Luogo: ENS, Parigi, Francia
- Luglio 2003: An Anonymous Credential System and a Privacy-Aware PKI
Ambito: Conferenza ACISP '03
Luogo: Wollongong, Australia
- Febbraio 2003: Authentication and Privacy on the Internet
Ambito: Difesa tesi di dottorato
Luogo: Dipartimento di Informatica ed Applicazioni, Baronissi (SA), Italia
- Settembre 2002: Privacy in Subscription-Based Services (seminario)
Ambito: Seminario settimanale dell'IBM
Luogo: IBM Zurich Research Laboratory - Ruschlikon, Svizzera

- Settembre 2002: A Format-Independent Architecture for Run-Time Integrity Checking of Executable Code
Ambito: Conferenza SCN '02
Luogo: Amalfi, Salerno, Italia

5 Attività Organizzative

- Organizzatore con Christian Cachin, Eyal Kushilevitz, Anna Lysyanskaya e Giuseppe Persiano del “Workshop on Protocols and Public-Key Cryptography” tenutosi a Bertinoro, dal 24 al 29 maggio 2009.
- General Co-Chair (in collaborazione con Roberto De Prisco) della conferenza: “The 6th Conference on Security and Cryptography for Networks (SCN 2008)” - (10 - 12 settembre 2008) - Amalfi, Italia, proceedings LNCS Vol 5229, Springer-Verlag.
- Organizzatore del Provilab (ECRYPT) Meeting on Cryptographic Protocols, tenutosi a Salerno, dal 24 al 26 ottobre 2007.
- Organizzatore insieme con Giuseppe Persiano della ECRYPT Autumn International PhD School on Zero-Knowledge Foundations and Applications, 29 Ottobre - 2 Novembre 2006, Università di Bologna, Centro Residenziale di Bertinoro (Forlì), Italia.
- Organizzatore del Provilab (ECRYPT) Meeting on Secure and Practical Protocols, tenutosi a Roma dal 28 al 30 settembre 2005.

6 Direzione/Partecipazione di/in Gruppi di Ricerca e Grant

- Coordinatore del progetto: “Progettazione ed implementazione di un protocollo distribuito e di un sistema di navigazione sicuro e privato per l'esecuzione di transazioni sicure e private sul Web”. Il progetto è stato finanziato con fondi per giovani ricercatori nel 2001 dall'Università di Salerno.
- Coordinatore del progetto: “Token malleabili per l'accesso anonimo a servizi riservati”. Il progetto è stato finanziato con fondi per giovani ricercatori nel 2002 dall'Università di Salerno.
- Membro del Network of Excellence “ECRYPT” (commissione europea, sesto programma quadro, 2004-2008). Attività svolta per i gruppi di ricerca su crittografia asimmetrica (**AZTEC**) e protocolli (**PROVILAB**).
- Membro del Network of Excellence “ECRYPT II” (commissione europea, settimo programma quadro, 2008-2012). Attività svolta per i gruppi **MAYA** e **SYMLAB**.

- Membro dello Specific Targeted Research Project (STREP) “FRONTS” (commissione europea, settimo programma quadro, 2007-2011). Attività svolta per i gruppi di ricerca WP2 “Adapting the Network Infrastructure” e WP6 “Dissemination, Collaboration and Exploitation”.
- Membro dell’Integrated European Project “AEOLUS” (commissione europea, sesto programma quadro, 2006-2009). Attività svolta per i gruppi di ricerca su **Security and trust management**.
- Dal 2005, membro dell’International Association for Cryptologic Research (IACR).
- Dal 2005, per svariati anni membro della European Association for Theoretical Computer Science (EATCS).
- Dal 2008, per svariati anni membro del capitolo italiano dell’EATCS.
- Membro di diversi progetti FARB ex-60% dal 2000 al 2011.
- Membro del progetto “Sistemi Crittografici per Preservare la Privacy con Hardware di Sicurezza” finanziato dall’ateneo Italo-Tedesco nell’ambito del programma di scambio Vigoni, tra Università di Salerno e Ruhr-University Bochum (Germania), per il periodo 2009-2010.
- Membro del PRIN (Progetti di Ricerca di Interesse Nazionale) 2010-2012 dal titolo “Progettazione ed analisi di protocolli crittografici per la tutela della privacy PERSONALE E DEI DATI in basi di dati e dispositivi mobili (Design and analysis of cryptographic protocols safeguarding PERSONAL AND DATA privacy in databases and mobile computing).
- Membro del progetto “Protocolli Efficienti per il Two Party Secure Text-Processing”, finanziato dal GNCS (Gruppo Nazionale per il Calcolo Scientifico) per il 2011, in collaborazione con l’università degli studi di Catania.
- Responsabile scientifico del progetto “Sicurezza e Privacy per RFID e Reti di Sensori ” presentato per il bando per la partecipazione alla selezione ai progetti di Ricerca Scientifica della Regione Campania, finanziabili ai sensi della L.R. N. 5 del 28/03/2002. Il progetto è stato dichiarato finanziabile ma non finanziato per esaurimento risorse.
- Marzo 2009 - Ottenuto un grant della provincia di Salerno per la mobilità internazionale dei giovani ricercatori; il grant ha supportato la visita di 6 mesi presso UCLA (USA) da Agosto 2009 a Gennaio 2010.

7 Presentazioni su Invito

1. Presentazione su invito per lo STAR (Seminar on Theory, Algorithms and cRyptography Research) seminar at UCSD, La Jolla (CAL), USA.

2. Presentazione su invito per il Distinguished Lecturer Seminar Series at UCI, Irvine (CAL), USA.
3. Presentazione su invito per l'evento "Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference II" tenutosi a Lake Arrowhead (CAL), USA, giugno 2009.
4. Presentazione su invito al "Workshop on Cryptographic Protocols and Public-Key Cryptography", Bertinoro, Italia, maggio 2009.
5. Presentazione su invito nell'ambito del programma "Microsoft Research Colloquium '08", Redmond, USA, novembre 2008.
6. Presentazione su invito al Workshop "Security Hardware in Theory and Practice – A Marriage of Convenience" tenutosi a Dagstuhl, Germania, giugno 2008.
7. Presentazione su invito per l'evento "Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference I" tenutosi a Lake Arrowhead (CAL), USA, giugno 2008.
8. Presentazione su invito al Workshop on Cryptographic Protocols (WCP 2007), tenutosi a Bertinoro, Forlì nel mese di Marzo 2007, con titolo "Secure Proof Systems Under Man-in-the-Middle Attacks".
9. Presentazione su invito al Workshop Foundations of secure multi-party computation and zero-knowledge and its applications, tenutosi a Los Angeles, USA nel mese di Novembre 2006, con titolo "Concurrent Non-Malleable Witness Indistinguishability".

8 Comitati di Programma

1. **Program Chair** di "The 8th Conference on Security and Cryptography for Networks (SCN 2012)" - Amalfi, Italia - *LNCS Springer-Verlag (TBC)*.
2. PC member di "The 31st Advances in Cryptology (EUROCRYPT 2012)" - Cambridge, United Kingdom - **IACR** - *LNCS Springer-Verlag*.
3. PC member di "The 15th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2012)" - Darmstadt, GERMANY - **IACR** - *LNCS Springer-Verlag*.
4. PC member di "The 14th Information Security Conference (ISC 2011)" - Xi'an, China. - *LNCS Springer-Verlag*.
5. PC member di "The 10th International Conference on CRYPTOLOGY AND NETWORK SECURITY (CANS 2011)" - Sanya, China. - *LNCS Springer-Verlag*.
6. PC member di "The 9th International Conference on Applied Cryptography and Network Security (ACNS 2011)" - Malaga, Spain. - *LNCS Springer-Verlag*.

7. PC member di “The 4th International Conference on Cryptology AFRICACRYPT 2011”, Dakar, Senegal. - *LNCS Springer-Verlag*.
8. Membro del Program Committee della conferenza “The 9th International Conference on CRYPTOLOGY AND NETWORK SECURITY (CANS 2010)”. - Kuala Lumpur, Malaysia - *LNCS Springer-Verlag*.
9. Membro del Program Committee della conferenza “The 13th Information Security Conference (ISC 2010)” - Boca Raton, FL, USA - *LNCS Springer-Verlag*.
10. Membro del Program Committee della conferenza “The 7th Conference on Security and Cryptography for Networks (SCN 2010)” - Amalfi, Italia - *LNCS Springer-Verlag*.
11. Membro del Program Committee della conferenza “The 13th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2010)” - Parigi, Francia - **IACR** - *LNCS Springer-Verlag*.
12. Membro del Program Committee della conferenza “The 8th International Conference on CRYPTOLOGY AND NETWORK SECURITY (CANS 2009)”. - Kanazawa, Ishikawa, Japan - *LNCS Springer-Verlag*.
13. Membro del Program Committee della conferenza “The 15th Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2009)”. - Tokio, Japan - **IACR** - *LNCS Springer-Verlag*.
14. Membro del Program Committee della conferenza “The 12th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2009)” - Irvine (CAL), USA - **IACR** - *LNCS Springer-Verlag*.
15. Membro del Program Committee della conferenza “The 6th Conference on Security and Cryptography for Networks (SCN 2008)” - Amalfi, Italia - *LNCS Springer-Verlag*.
16. Membro del Program Committee della conferenza “RSA Conference 2006, Cryptographers’ Track (RSA 2006)” - San Jose, USA - *LNCS Springer-Verlag*.
17. Membro del Program Committee della conferenza “The 2nd Conference on Information Security and Cryptology (INSCRYPT 2006)” - Pechino, Cina, *LNCS Springer-Verlag*.
18. Membro del Program Committee della conferenza “The 1st Conference on Trust and Privacy in Digital Business (TrustBus 2004)” - Saragozza (Spagna) - *LNCS Springer-Verlag*.

9 Direzioni di Sessioni

1. Session Chair della sessione “Cryptographic Protocols I” per la conferenza “The 7th Conference on Security and Cryptography for Networks (SCN 2010)”, Amalfi (Italia) - *LNCS Springer-Verlag*.

2. Session Chair della sessione “Models and Frameworks I” per la conferenza “The 15th Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2009)” - Tokio, Japan - **IACR** - *LNCS Springer-Verlag*.
3. Session Chair della sessione “Applications and Protocols” per la conferenza “The 12th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2009)”, - Irvine (CAL), USA - **IACR** - *LNCS Springer-Verlag*
4. Session Chair della sessione “Encryption 3” per la conferenza “The 6th Conference on Security and Cryptography for Networks (SCN 2008)”, Amalfi (Italia) - *LNCS Springer-Verlag*.
5. Session Chair della sessione “Encryption 2” per la conferenza “The 6th Conference on Security and Cryptography for Networks (SCN 2008)”, Amalfi (Italia) - *LNCS Springer-Verlag*.
6. Session chair per “Secure Computation” in “The 35th International Colloquium on Automata, Languages and Programming (ICALP 2008)”, Reykjavik (Islanda) - **EATCS** - *LNCS Springer-Verlag*.
7. Session chair per “Protocols” per il “Workshop on Secure Component and System Identification (SECSI 2008)”, Berlino (Germania).
8. Session chair per “Mobile and Network Security (2)” in “The 8th Australasian Conference on Information Security and Privacy (ACISP 2003)”, Wollongong (Australia) - *LNCS Springer-Verlag*.

10 Studi ed Incarichi Ricoperti

- Da Ottobre 2010: In visita per presso il Computer Science Department, University of California at Los Angeles (UCLA), Los Angeles, USA.
- Agosto 2010 - In visita per una settimana presso il System Security Group, Horst Görtz Institute for IT-Security, Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germania.
- Febbraio 2010 - In visita per una settimana presso il System Security Group, Horst Görtz Institute for IT-Security, Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germania.
- Da Agosto 2009 a Gennaio 2010: In visita per 6 mesi presso il “Center for Information and Computation Security”, Computer Science Department, University of California at Los Angeles (UCLA), Los Angeles, USA.
- Dicembre 2008 - In visita per due settimane presso il System Security Group, Horst Görtz Institute for IT-Security, Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germania.

- Novembre 2008 - In visita per una settimana presso il Microsoft Research Center, Redmond, USA.
- Agosto 2008 - In visita per una settimana presso il “Center for Information and Computation Security”, Los Angeles, USA.
- Febbraio 2008 - In visita per una settimana presso il System Security Group, Horst Görtz Institute for IT-Security, Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germania.
- Novembre 2006: Ho partecipato per 3 settimane su invito del “Institute for Pure and Applied Mathematics (IPAM, UCLA)” al “Fall 2006 Program on Securing Cyberspace: Application and Foundations of Cryptography and Computer Security”, svoltosi presso IPAM, Los Angeles (CAL), USA.
- Da dicembre 2005: Membro del Dipartimento di Informatica ed Applicazioni “R.M. Capocelli” dell’Università degli Studi di Salerno.
- Dal 01/11/2005: In servizio come Ricercatore presso la Facoltà di Scienze Matematiche, Fisiche e Naturali dell’Università degli Studi di Salerno.
- 01/12/2004-31/10/2005 (11 mesi): Titolare di un assegno di ricerca biennale denominato “Criptologia” presso il Dipartimento di Informatica ed Applicazioni - Università di Salerno.
- 01/10/2003-30/09/2004 (1 anno): Ricercatore Post-Doc presso il “Complexity and Cryptography Research Group” del Département d’Informatique dell’ École Normale Supérieure, Parigi, Francia.
- 01/10/1999-30/09/2003 (4 anni): Titolare di un assegno per la collaborazione ad attività di ricerca denominato “Esperto di ottimizzazione” presso il Dipartimento di Informatica ed Applicazioni - Università di Salerno.
- 2003 (Febbraio): Conseguimento del titolo di *Dottore di Ricerca in Informatica* presso l’Università di Salerno.
Tesi : On Authentication and Privacy on the Internet.
Advisor : Prof. Giuseppe Persiano.
Chairman : Prof. Alfredo De Santis.
- 2002 (4 mesi): In visita presso l’IBM Zurich Research Laboratory (Ruschlikon, Svizzera) come ricercatore per un progetto comune tra l’IBM Zurich Research Laboratory e l’Università di Salerno. L’attività di ricerca è stata svolta in collaborazione con il dott. Christian Cachin su *Secure Replication of Services*.
- Dicembre 2001 - In visita per una settimana presso il Computer Technology Institute, Patrasso, Grecia.

- 1999 - 2002: Studente di dottorato di ricerca in Informatica dell'Università di Salerno. Concorso vinto classificandomi al primo posto.
- 1999 - 2003: Consulente e docente su varie tematiche tra cui Java, tecnologie per il WEB, Oracle e sicurezza su reti per Metoda s.p.a. - (Salerno), Getronics (ex Olivetti Ricerca) - (Pozzuoli (Napoli)), Lotus Development Italia - (Milano), S.D.S. Nuove Tecnologie (Roma), Diogene Consulenze Informatiche (Roma), Istituto P. Martini (Roma).
- Ottobre 1998: Conseguimento della laurea in informatica con voto 110/110 e lode presso l'Università di Salerno (**prima laurea in informatica rilasciata da questa università**).
Indirizzo : Reti Informatiche.
Titolo Tesi : Transazioni Anonime sul Web: Protocolli ed Implementazioni.
Relatore : Prof. Giuseppe Persiano.

Lingue straniere conosciute. Ottima conoscenza della lingua inglese, sia scritta che parlata. Conoscenze di base della lingua francese (sia scritta che parlata).

11 Collaborazioni con Studenti/Dottorandi

Christian Wachsmann. Ho svolto l'attività di relatore per la diploma thesis di Christian Wachsmann della Ruhr-University di Bochum (Germania), sull'utilizzo di RFID per l'e-ticketing relativo al trasporto. La collaborazione ha prodotto gli articolo "User Privacy in Transport Systems Based on RFID E-Tickets" [30, 33]. La collaborazione è ancora in corso, Christian è ora PhD student presso la Ruhr-University di Bochum (Germania) .

Abhishek Jain and Omkant Pandey. Nel periodo 2007-2010, ho condotto attività di ricerca con Abhishek Janin e Omkant Pandey che sono PhD student in computer science at the Department of Computer Science - University of California at Los Angeles (UCLA). La collaborazione si è incentrata su sicurezza rispetto ad attacchi man-in-the-middle. Tale attività ha prodotto una pubblicazione a TCC 2010 [39] ed altri articoli in preparazione [40, 41].

Joël Alwen. Nel periodo ottobre 2004-luglio 2005, ho condotto attività di ricerca con Joël Alwen che ricopriva la seguente posizione: student of Bachelor of Software and Information Engineering, Department of Computer Science - University of Vienna. Ho coordinato ed indirizzato in parte la sua attività di ricerca su protocolli zero knowledge. Tale attività ha prodotto una pubblicazione a CRYPTO 2005 [17].

Carmine Ventre. Nel periodo ottobre 2005-settembre 2007, ho condotto attività di ricerca con Carmine Ventre, che ha ricoperto le posizioni di dottorando in informatica e poi assegnista di ricerca presso il Dipartimento di Informatica ed Applicazioni dell'Università di Salerno. Ho coordinato ed indirizzato in parte la sua attività di ricerca su schemi di cifratura. Tale attività ha prodotto una pubblicazione a PKC 2008 [24], un pubblicazione ad AFRICACRYPT 2009 [33] ed altri articoli in preparazione.

Luigi Catuogno. Nel periodo 2001-2005, ho condotto attività di ricerca con Luigi Catuogno, che ha ricoperto le posizioni di dottorando in informatica e poi tecnico presso il Dipartimento di Informatica ed Applicazioni dell'Università di Salerno. La collaborazione si è incentrata sull'esecuzione sicura di software e sicurezza in ambienti distribuiti. Tale attività ha prodotto le seguenti pubblicazioni: [3, 6, 9, 12, 18].

Alessandra Scafuro. Nel 2009 ho supervisionato la tesi di laurea di Alesandra Scafuro sulle nozioni di sicurezza e privacy per la tecnologia RFID. La collaborazione ha prodotto pubblicazioni ad RFIDSec 2009 and ALGOSENSORS 2009 [35, 37]. Alessandra Scafuro è attualmente svolge il dottorato di ricerca all'università di Salerno sotto la mia supervisione.

Sanjam Garg and Akshay Wadia. Nel 2009 durante la mia visita di 6 mesi ad UCLA ho collaborato con Sanjam Garg and Akshay Wadia, entrambi col ruolo di PhD student in computer science presso il Department of Computer Science - University of California at Los Angeles (UCLA), su protocolli per Resettable Zero Knowledge. La collaborazione ha prodotto un articolo in preparazione.

Zongyang Zhang. Nel periodo 2009-2010 ho collaborato con Zongyang Zhang, PhD student del Department of Computer Science and Engineering Shanghai Jiao Tong University, su non-malleable commitments. La collaborazione ha prodotto un articolo pubblicato a PKC 2010 [42].

Claudio Orlandi. Nel periodo 2009-2010 ho collaborato con Claudio Orlandi, PhD student presso il Department of Computer Science, Aarhus Univeristy, su non-malleable zero knowledge. La collaborazione ha prodotto un articolo in preparazione.

Altre collaborazioni con studenti. Ulteriori progetti di ricerca sono stati avviati con Joshua Baron (UCLA), Angelo De Caro (Univ. Salerno), Emiliano De Cristofaro (UCI), Vanishree HRao (UCLA), Abishek Kumarasubramanian (UCLA), Chen-Kuei Lee (UCLA), Silas Richelson (UCLA), Thomas Schneider (Univ. Bochum) e Chongwon Wong (UCLA).

12 Altre Attività Scientifiche

1. Editor insieme con Rafail Ostrovsky e Roberto De Prisco, dei proceedings relativi alla conferenza "The 6th Conference on Security and Cryptography for Networks (SCN 2008)" - (10 - 12 settembre 2008) - Amalfi, Italia, proceedings LNCS, Vol. 5229, Springer-Verlag, Heidelberg, Germania, Agosto 2008, ISBN 978-3-540-85854-6, [1].
2. Editor dei deliverable "Summary Report on Models and Definitions for Cryptographic Protocols" del 2008, e "Second Summary Report on Two-Party Protocols" del 2006, del gruppo di ricerca PROVILAB WG1 del network of excellence ECRYPT.

3. Ho contribuito al deliverable “Lightweight Cryptographic Algorithms” prodotto dal working group WG2 del 2010 per il gruppo di ricerca SYMLAB, al deliverable “New Technical Trends in Asymmetric Cryptography” prodotto dal working group WG3 del 2007 per il gruppo di ricerca AZTEC, del deliverable “Rational Cryptographic Protocols” del 2007 del gruppo di ricerca PROVILAB, del deliverable prodotto dal working group WG3 del 2005 per il gruppo di ricerca AZTEC, del deliverable “First Summary Report on Two-Party Protocols” del 2005 del gruppo di ricerca PROVILAB WG1, il tutto nell’ambito delle attività del network of excellence ECRYPT.
4. Ho svolto/sto svolgendo attività di referaggio per le seguenti conferenze e riviste internazionali:

Riviste: ACM TISSEC, Journal of Cryptology, ACM Computing Surveys, International Journal of Information Security, Journal of Systems and Software, Journal of Computer Science and Technology, Information Processing Letters, Journal of Mathematical Cryptology (JMC), Theoretical Computer Science (TCS), Electronics and Telecommunications Research Institute Journal (ETRI), IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Transactions on Computational Science.

Conferenze: TCC 2011, EUROCRYPT 2011, ACNS 2011, AFRICACRYPT 2011, PKC 2011, CRYPTO 2011, ICALP 2011, FOCS 2011, MFCS 2011, PROVSEC 2011, ASIACRYPT 2011, ISC 2011, CANS 2011, PKC 2010, SCN 2010, FOCS 2010, MFCS 2010, ISC 2010, CANS 2010, CRYPTO 2010, ICALP 2010, EUROCRYPT 2010, TCC 2010, PKC 2010, STACS 2010, ESORICS 2010, SCN 2010, INSCRYPT 2010, CRYPTO 2009, EUROCRYPT 2009, TCC 2009, ASIACRYPT 2009, PKC 2009, MFCS 2009, ISC 2009, ALGOSENSORS 2009, ICITS 2009, ACNS 2009, AFRICACRYPT 2009, INSCRYPT 2009, CANS 2009, INSCRYPT 2008, FOCS 2008, ASIACRYPT 2008, ICISC 2008, ICICS 2008, CANS 2008, ICITS 2008, SIROCCO 2008, ICALP 2008, ASIACCS 2008, Financial Cryptography 2008, ICISC 2007, Secrypt 2007, Inscrypt 2007, CRYPTO 2007, FUN 2007, ICALP 2007, EUROCRYPT 2007, TCC 2007, PKC 2007, Cryptology Eprint Archive 2006/2007, INSCRYPT 2006, CANS 2006, AlgoSensor 2006, CMS 2006, SCN 2006, ACISP 2006, ICALP 2006, DSN 2006, PKC 2006, STOC 2006, CISC 2005, ISC 2005, RSA 2006, ICICS 2005, WISA 2005, CMS 2005, ICALP 2005, PODS 2005, STACS 2005, SIROCCO 2005, DSN 2005, SCN 2004, CSES 2004, WISA 2004, ASIACRYPT 2004, FOCS 2004, TrustBus 2004, ISCC 2004, WISA 2003, CIAC 2003, ICTCS 2001, CRYPTO 2001.

13 Attività Applicative - Convenzioni di Dipartimento

Le seguenti attività riguardano specifici progetti culminati in sviluppo di sistemi realmente implementati. Non riguardano lavori fatti dagli studenti durante le attività di tirocinio sotto la mia supervisione.

- 2000 Implementazione (in C) di una libreria (Moz2i) per la gestione di chiavi e certificati digitali del database di Netscape. Sorgenti e documentazione sono disponibili sul web al seguente

URL:

<http://www.dia.unisa.it/visconti/SPSL/>.

2000 Progettazione ed implementazione di una API (in C) per il protocollo SPSL, di un proxy col supporto di SPSL e di un modulo per il web server Apache col supporto di SPSL. Sorgenti disponibili sul web:

<http://www.dia.unisa.it/visconti/SPSL/>.

2002 Progettazione ed implementazione di un'architettura per il controllo dell'integrità degli eseguibili a run time. Per la realizzazione di tale architettura sono stati progettati ed implementati (tra l'altro) alcuni moduli per il kernel di Linux. Sorgenti disponibili sul web:

<http://wlf.dia.unisa.it>.

2002 Studio di fattibilità e realizzazione di un prototipo per una piattaforma per l'e-commerce utilizzando software open-source. Tale attività è stata svolta nell'ambito di una **convenzione** tra il Dipartimento di Informatica ed Applicazioni dell'università di Salerno ed STT s.p.a.

2003 Progettazione ed Implementazione di una piattaforma scalabile per l'e-commerce utilizzando software open-source. Il fulcro di tale piattaforma è un modulo per il web server Apache che interagisce con il DBMS MySQL ed i moduli PHP ed SSL. Tale attività è stata svolta nell'ambito di una **convenzione** tra il Dipartimento di Informatica ed Applicazioni dell'università di Salerno ed STT s.p.a.

2007 Progettazione ed Implementazione di un sistema sicuro di aggiornamento remoto del software, basato su Python-Twisted, OpenSSL, FreeBSD, nell'ambito di una **convenzione** tra il Dipartimento di Informatica ed Applicazioni dell'università di Salerno e Bit4ID.

14 Partecipazione a Workshop/Conferenze e Meeting

Ho partecipato alle seguenti conferenze e meeting internazionali:

- *Titolo:* The 8th Theory of Cryptography Conference - TCC 2011 - Conferenza
Data: Marzo 2011
Luogo: Providence, USA
- *Titolo:* Mathematics of Information-Theoretic Cryptography - Workshop
Data: Marzo 2011
Luogo: Los Angeles, USA
- *Titolo:* ECRYPT II Network of Excellence SYMLAB Meeting
Data: Settembre 2010
Luogo: Leuven, Belgio

- *Titolo:* European Crypto Day
Data: Settembre 2010
Luogo: Leuven, Belgio
- *Titolo:* The 7th Conference on Security and Cryptography for Networks - SCN 2010 - Conferenza
Data: Settembre 2010
Luogo: Amalfi, Italia
- *Titolo:* Advances in Cryptology - CRYPTO 2010 - Conferenza
Data: Agosto 2010
Luogo: Santa Barbara, California, USA
- *Titolo:* Advances in Cryptology - EUROCRYPT 2010 - Conferenza
Data: Maggio 2010
Luogo: Montecarlo, Monaco
- *Titolo:* Lattice Crypto Day - Workshop
Data: Maggio 2010
Luogo: Paris, France
- *Titolo:* The 13th International Workshop on Practice and Theory in Public Key Cryptography - PKC 2010 - Conferenza
Data: Maggio 2010
Luogo: Paris, France
- *Titolo:* ECRYPT II Network of Excellence MAYA Meeting
Data: Maggio 2009
Luogo: Zurigo, Svizzera
- *Titolo:* The 7th Theory of Cryptography Conference - TCC 2010 - Conferenza
Data: Febbraio 2010
Luogo: Zurigo, Svizzera
- *Titolo:* Advances in Cryptology - ASIACRYPT 2009 - Conferenza
Data: Dicembre 2009
Luogo: Tokyo, Giappone
- *Titolo:* Advances in Cryptology - CRYPTO 2009 - Conferenza
Data: Agosto 2009
Luogo: Santa Barbara, California, USA
- *Titolo:* ECRYPT II Network of Excellence MAYA Meeting
Data: Giugno 2009
Luogo: Losanna, Svizzera

- *Titolo:* The 2nd International Conference on the Theory and Applications of Cryptology - AFRICACRYPT 2009 - Conferenza
Data: Giugno 2009
Luogo: Gammarth, Tunisia
- *Titolo:* Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference II
Data: Giugno 2009
Luogo: Lake Arrowhead (CAL), USA
- *Titolo:* Workshop on Cryptographic Protocols and Public-Key Cryptography - WCP 2009 - Workshop
Data: Maggio 2009
Luogo: Bertinoro, Forlì, Italia
- *Titolo:* The 12th International Workshop on Practice and Theory in Public Key Cryptography - PKC 2009 - Conferenza
Data: Marzo 2009
Luogo: Irvine, USA
- *Titolo:* The 6th Theory of Cryptography Conference - TCC 2009 - Conferenza
Data: Marzo 2009
Luogo: San Francisco, USA
- *Titolo:* ECRYPT II Network of Excellence Kick-off Meeting
Data: Novembre 2008
Luogo: Leuven, Belgio
- *Titolo:* International Workshop on Privacy in Location-Based Applications - PILBA 2008 - Workshop
Data: Ottobre 2008
Luogo: Malaga, Spagna
- *Titolo:* The 13th European Symposium on Research in Computer Security - ESORICS 2008 - Conferenza
Data: Ottobre 2008
Luogo: Malaga, Spagna
- *Titolo:* The 6th Conference on Security and Cryptography for Networks - SCN 2008 - Conferenza
Data: Settembre 2008
Luogo: Amalfi, Italia
- *Titolo:* Advances in Cryptology - CRYPTO 2008 - Conferenza
Data: Agosto 2008
Luogo: Santa Barbara, California, USA

- *Titolo:* Foundations of Information Management in Networks - Workshop
Data: Luglio 2008
Luogo: Reykjavik, Islanda
- *Titolo:* The 35th International Colloquium on Automata, Languages and Programming - ICALP 2008 - Conferenza
Data: Luglio 2008
Luogo: Reykjavik, Islanda
- *Titolo:* Provilab (ECRYPT) Meeting on Secure Protocols - Meeting
Data: Giugno 2008
Luogo: Berlino, Germania
- *Titolo:* Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference I
Data: Giugno 2008
Luogo: Lake Arrowhead (CAL), USA
- *Titolo:* Security Hardware in Theory and Practice A Marriage of Convenience (Giugno 2008, Dagstuhl - Germania
Data: Giugno 2008
Luogo: Dagstuhl, Germania
- *Titolo:* The 1st Workshop on Secure Component and System Identification - SECSI 2008 - Conferenza
Data: Marzo 2008
Luogo: Berlino, Germania
- *Titolo:* The 11th International Workshop on Practice and Theory in Public Key Cryptography - PKC 2008 - Conferenza
Data: Marzo 2008
Luogo: Barcellona, Spagna
- *Titolo:* Tenth Italian Conference on Theoretical Computer Science - ICTS 2007 - Conferenza
Data: Ottobre 2007
Luogo: Roma, Italia
- *Titolo:* Advances in Cryptology - CRYPTO 2007 - Conferenza
Data: Agosto 2007
Luogo: Santa Barbara, California, USA
- *Titolo:* AZTEC (ECRYPT) Meeting on Proxy Encryption - Meeting
Data: Giugno 2007
Luogo: Firenze, Italia

- *Titolo:* Second Italian Workshop on PRIVacy and SEcurity - PRISE 2007
Data: Giugno 2007
Luogo: Roma, Italia
- *Titolo:* Advances in Cryptology - EUROCRYPT 2007 - Conferenza
Data: Maggio 2007
Luogo: Barcellona, Spagna
- *Titolo:* Provilab (ECRYPT) Meeting on Concrete Security - Meeting
Data: Marzo 2007
Luogo: Louvain-la-Neuve, Belgio
- *Titolo:* Workshop on Cryptographic Protocols - WCP 2007 - Workshop
Data: Marzo 2007
Luogo: Bertinoro, Forlì, Italia
- *Titolo:* The 4th Theory of Cryptography Conference - TCC 2007 - Conferenza
Data: Marzo 2007
Luogo: Amsterdam, Paesi Bassi
- *Titolo:* Infosecurity 2007 - Serie di Convegni
Data: Febbraio 2007
Luogo: Milano, Italia
- *Titolo:* Foundations of secure multi-party computation and zero-knowledge and its applications - Workshop
Data: Novembre 2006
Luogo: UCLA, Los Angeles, USA
- *Titolo:* Provilab (ECRYPT) Meeting on Anonymous Credentials - Meeting
Data: October 2006
Luogo: Bochum, Germania
- *Titolo:* The 5th Conference on Security and Cryptography for Networks - SCN 2006 - Conferenza
Data: Settembre 2006
Luogo: Maiori, Italia
- *Titolo:* The 31st International Symposium on Mathematical Foundations of Computer Science - MFCS 2006 - Conferenza
Data: Agosto 2006
Luogo: Stará Lesná, Slovacchia
- *Titolo:* The 33rd International Colloquium on Automata, Languages and Programming - ICALP 2006 - Conferenza
Data: Luglio 2006
Luogo: Venezia, Italia

- *Titolo:* Advances in Cryptology - EUROCRYPT 2006 - Conferenza
Data: Maggio 2006
Luogo: San Pietroburgo, Russia
- *Titolo:* Provilab (ECRYPT) Meeting on Game Theory and Cryptography - Meeting
Data: Aprile 2006
Luogo: Eindhoven, Paesi Bassi
- *Titolo:* The 3rd Theory of Cryptography Conference - TCC 2006 - Conferenza
Data: Marzo 2006
Luogo: New York, USA
- *Titolo:* Provilab (ECRYPT) Meeting on Secure and Practical Protocols - Meeting
Data: Settembre 2005
Luogo: Roma, Italia
- *Titolo:* The 32nd International Colloquium on Automata, Languages and Programming - ICALP 2005 - Conferenza
Data: Luglio 2005
Luogo: Lisbona, Portogallo
- *Titolo:* Advances in Cryptology - EUROCRYPT 2005 - Conferenza
Data: Maggio 2005
Luogo: Aarhus, Danimarca
- *Titolo:* Provilab (ECRYPT) Meeting on Protocol Composition - Meeting
Data: Aprile 2005
Luogo: Zurigo, Svizzera
- *Titolo:* Advances in Cryptology - ASIACRYPT 2004 - Conferenza
Data: Dicembre 2004
Luogo: Jeju island, Corea
- *Titolo:* ECRYPT (Provilab) 2004 - Meeting
Data: Novembre 2004
Luogo: Roma, Italia
- *Titolo:* CRESCCO 2004 - WORKSHOP
Data: Ottobre 2004
Luogo: Roma, Italia
- *Titolo:* Advances in Cryptology - CRYPTO 2004 - Conferenza
Data: Agosto 2004
Luogo: Santa Barbara, California, USA

- *Titolo:* Advances in Cryptology - EUROCRYPT 2004 - Conferenza
Data: Maggio 2004
Luogo: Interlaken, Svizzera
- *Titolo:* 8th International Financial Cryptography Conference (FC 2004) - Conferenza
Data: Febbraio 2004
Luogo: Key West, Florida, USA
- *Titolo:* 8th Australasian Conference on Information Security and Privacy (ACISP 2003) - Conferenza
Data: Luglio 2003
Luogo: Wollongong, Australia
- *Titolo:* 5th Conference on Algorithms and Complexity (CIAC 2003) - Conferenza
Data: Maggio 2003
Luogo: Università "La Sapienza", Roma, Italia
- *Titolo:* 3rd Conference on Security in Communication Networks (SCN 2002) - Conferenza
Data: Settembre 2002
Luogo: Amalfi (SA), Italia
- *Titolo:* 33rd Annual ACM Symposium on Theory of Computing (STOC 2001) - Conferenza
Data: Luglio 2001
Luogo: Creta, Grecia

15 Articoli Scientifici

15.1 Volumi

Elenco dei volumi di cui sono editor:

- 1 Proceedings of the Sixth Conference on Security and Cryptography for Networks (**SCN 2008**).
10-12 Settembre 2008, Amalfi (SA), Italia.
Lecture Notes in Computer Science Vol. 5229, Springer-Verlag, Heidelberg, ISBN 978-3-540-85854-6, Agosto 2008.
Autori: Rafail Ostrovsky, Roberto De Prisco, Ivan Visconti.

15.2 Riviste

Elenco pubblicazioni in riviste (in ordine cronologico):

- 2 A Secure and Private System for Subscription-Based Remote Services.
ACM Transactions on Information and System Security (**TISSEC**), Vol. 6, Num. 4, Pagg. 472-500, ACM Press New York, NY, USA . November 2003, ISSN:1094-9224.
Autori: Pino Persiano, Ivan Visconti.

- 3 An Architecture for Verification of Executables at Run Time.
The Computer Journal, British Computer Society (**TCJ**), 1 Sanford Street Swindon Wiltshire United Kingdom SN1 1HJ, Vol. 47, Num. 5, Pagg. 511-526, September 2004, ISSN:0010-4620.
Autori: Luigi Catuogno, Ivan Visconti.
- 4 Hybrid Commitments and their Applications to Zero-Knowledge Proof Systems.
Theoretical Computer Science, Elsevier (**TCS**), vol. 374, pp. 229-260, April 2007, ISSN: 0304-3975.
Autori: Dario Catalano, Ivan Visconti.
- 5 Impossibility Results for RFID Privacy Notions.
Transactions on Computational Science XI - Special Issue on Security in Computing, Part II (**Springer TCS**). vol. 11, pp. 39-63, 2010, Lecture Notes in Computer Science 6480 Springer, ISBN 978-3-642-17696-8.
Autori: Frederik Armknecht, Ahmad-Reza Sadeghi, Alessandra Scafuro, Ivan Visconti, Christian Wachsmann.
- 6 On Constant-Round Concurrent Non-Malleable Proof Systems.
Information Processing Letters, Elsevier (**IPL**), vol. 111, pp. 883-890, September 2011, ISSN: 0020-0190.
Autori: Zhenfu Cao, Ivan Visconti, Zongyang Zhang.

15.3 Atti di Convegni

Elenco pubblicazioni in conferenze (in ordine cronologico):

- 7 User Privacy Issues Regarding Certificates and the TLS protocol: the Design and Implementation of the SPSL protocol.
In proceedings of the Seventh ACM Conference on Communications and Security (**CCS 2000**). Pagg. 53-62. Novembre 1-4, 2000, Atene, Grecia. ACM Press, New York, NY, USA, October 2000, ISBN:1-58113-203-4.
Autori: Pino Persiano, Ivan Visconti.
- 8 A Format-Independent Architecture for Run-Time Integrity Checking of Executable Code.
In proceedings of the Third Conference on Security in Communication Networks (**SCN 2002**). 11-13 Settembre 2002, Amalfi (SA), Italia.
Lecture Notes in Computer Science Vol. 2576, Pagg. 219-233, Springer-Verlag, Heidelberg, Germania, 2003, ISBN: 3-540-00420-3.
Autori: Luigi Catuogno, Ivan Visconti.
- 9 An Anonymous Credential System and a Privacy-Aware PKI.
In proceedings of the Eighth Australasian Conference on Information Security and Privacy (**ACISP 2003**). 9-11 Luglio 2003, Wollongong, Australia.
Lecture Notes in Computer Science Vol. 2727, Pagg. 27-38, Springer-Verlag, Heidelberg,

- Germania, 2003, ISBN: 3-540-40515-1.
Autori: Pino Persiano, Ivan Visconti.
- 10 Anonymous Group Communication in Mobile Networks.
In proceedings of the Eighth Italian Conference on Theoretical Computer Science (**ICTCS 03**). 13-15 Ottobre 2003, Bertinoro, Italia.
Lecture Notes in Computer Science Vol. 2841, Pagg. 316-328, Springer-Verlag, Heidelberg, Germania 2003, ISBN: 3-540-20216-1.
Autori: Stelvio Cimato, Paolo D'Arco, Ivan Visconti.
- 11 A Lightweight Security Model for WBEM.
In proceedings of Workshop on Reliable and Secure Middleware (**WRSM 03**). 3-7 Novembre 2003, Catania, Italia.
Lecture Notes in Computer Science Vol. 2889, Pagg. 975-988, Springer-Verlag, Heidelberg, Germania, 2003, ISBN: 3-540-20494-6.
Autori: Giuseppe Cattaneo, Luigi Catuogno, Umberto Ferraro Petrillo, Ivan Visconti.
- 12 An Efficient and Usable Multi-Show Non-Transferable Anonymous Credential System.
In proceedings of the Eighth International Financial Cryptography Conference (**FC 04**). 9-12 Febbraio 2004, Key West, Florida, USA.
Lecture Notes in Computer Science, Vol. 3110, Pagg. 196-211, Springer-Verlag, Heidelberg, Germania, 2004, ISBN: 3-540-22420-3.
Autori: Giuseppe Persiano, Ivan Visconti.
- 13 Constant-Round Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model.
In proceedings of the Twenty-Fourth Annual IACR Crypto Conference (**CRYPTO 04**). August 15-19, 2004, Santa Barbara, USA.
Lecture Notes in Computer Science, Vol. 3152, Pagg. 237-253, Springer-Verlag, 2004, Heidelberg, Germania, ISBN 3-540-22668-0.
Autori: Giovanni Di Crescenzo, Giuseppe Persiano, Ivan Visconti.
- 14 Reliable Accounting in Grid Economic Transactions.
In proceedings of Workshop on Information Security and Survivability for Grid (**GISS 04**). 21-24 Ottobre 2004, Wuhan, Cina.
Lecture Notes in Computer Science, Vol. 3252, Pagg. 514-521, ISBN 3-540-23578-7, 2004, Springer-Verlag, Heidelberg, Germania.
Autori: Luigi Catuogno, Pompeo Faruolo, Umberto Ferraro Petrillo, Ivan Visconti.
- 15 Improved Setup Assumptions for 3-Round Resettable Zero Knowledge.
In proceedings of the Tenth Annual IACR Asiacrypt Conference (**ASIACRYPT 04**). 5-9 Dicembre 2004, Jeju, Korea.
Lecture Notes in Computer Science, Vol. 3329, Pagg. 530-544, ISBN 3-540-23975-8, 2004, Springer-Verlag, Heidelberg, Germania.
Autori: Giovanni Di Crescenzo, Giuseppe Persiano, Ivan Visconti.

- 16 Concurrent Zero Knowledge in the Public-Key Model.
In proceedings of the 32nd International Colloquium on Automata, Languages and Programming (**ICALP 05**). July 11-15, 2005, Lisboa, Portugal.
Lecture Notes in Computer Science, Vol. 3580, Pagg. 816-827, ISBN 3-540-27580-0, 2005, Springer-Verlag, Heidelberg, Germania.
Autori: Giovanni Di Crescenzo, Ivan Visconti.
- 17 Hybrid Trapdoor Commitments and Their Applications.
In proceedings of the 32nd International Colloquium on Automata, Languages and Programming (**ICALP 05**). July 11-15, 2005, Lisboa, Portugal.
Lecture Notes in Computer Science, Vol. 3580, Pagg. 298-310, ISBN 3-540-27580-0, 2005, Springer-Verlag, Heidelberg, Germania.
Autori: Dario Catalano, Ivan Visconti.
- 18 Single-Prover Concurrent Zero Knowledge in Almost Constant Rounds.
In proceedings of the 32nd International Colloquium on Automata, Languages and Programming (**ICALP 05**). July 11-15, 2005, Lisboa, Portugal.
Lecture Notes in Computer Science, Vol. 3580, Pagg. 228-240, ISBN 3-540-27580-0, 2005, Springer-Verlag, Heidelberg, Germania.
Autori: Giuseppe Persiano, Ivan Visconti.
- 19 Impossibility and Feasibility Results for Zero Knowledge with Public Keys.
In proceedings of the Twenty-Fifth Annual IACR Crypto Conference (**CRYPTO 05**). August 14-18, 2005, Santa Barbara, USA.
Lecture Notes in Computer Science, Vol. 3621, Pagg. 135-151, ISBN: 3-540-28114-2, 2005, Springer-Verlag, Heidelberg, Germania.
Autori: Joël Alwen, Giuseppe Persiano, Ivan Visconti.
- 20 Securing Operating System Services Based on Smart Cards.
In proceedings of the Second International Conference on Trust, Privacy, and Security in Digital Business (**TRUSTBUS 05**). August 22-26, 2005, Copenhagen, Denmark.
Lecture Notes in Computer Science, Vol. 3592, Pagg. 321-330, ISBN: 3-540-28224-6, 2005, Springer-Verlag, Heidelberg, Germania.
Autori: Luigi Catuogno, Roberto Gassirà, Michele Masullo, Ivan Visconti.
- 21 Mercurial Commitments: Minimal Assumptions and Efficient Constructions, In proceedings of the 3rd Theory of Cryptography Conference (**TCC 2006**). March 4-7 2006, New York, NY USA.
Lecture Notes in Computer Science, Vol. 3876, Pagg. 120-144, Springer-Verlag, 2006, ISBN: 3-540-32731-8, Heidelberg, Germania.
Autori: Dario Catalano, Yevgeniy Dodis, Ivan Visconti.
- 22 Efficient Zero Knowledge on the Internet, In proceedings of the 33rd International Colloquium on Automata, Languages and Programming (**ICALP 06**). July 9-16, 2006, Venezia, Italia.

- Lecture Notes in Computer Science, Vol. 4052, Pagg. 22-33, ISBN 3-540-35907-9, 2006, Springer-Verlag, Heidelberg, Germania.
Autori: Ivan Visconti.
- 23 On Non-Interactive Zero-Knowledge Proofs of Knowledge in the Shared Random String Model.
In proceedings of the 31st International Symposium on Mathematical Foundations of Computer Science (**MFCS 06**). August 28 - September 1, 2006, Stara Lesna, Slovak.
Lecture Notes in Computer Science, Vol 4162, Pagg. 753-764, ISBN 3-540-37791-3, 2006, Springer-Verlag, Heidelberg, Germania.
Autori: Giuseppe Persiano, Ivan Visconti.
- 24 PassePartout Certificates.
Second Italian Workshop on PRiVacy and SEcurity (**PRISE 2007**), June 6, 2007, Rome, Italy.
Autori: Ivan Visconti.
- 25 On Defining Proofs of Knowledge in the Bare Public-Key Model.
In proceedings of the 10th Italian Conference in Theoretical Computer Science (**ICTCS 2007**), October 3-5, 2007.
World Scientific, ISBN 981-277-098-4, 2007. Autori: Giovanni di Crescenzo, Ivan Visconti.
- 26 Completely Non-Malleable Encryption Revisited.
In proceedings of the Workshop on Public-Key Cryptography (**PKC 2008**), March 9-12, 2008.
Lecture Notes in Computer Science, Vol. 4939, Pagg. 65-84, Springer-Verlag, 2008, ISBN 3-540-78439-X Heidelberg, Germania.
Autori: Carmine Ventre, Ivan Visconti.
- 27 Identification Protocols Revisited - Episode I: E-Passports.
In Secure Component and System Identification (**SECSI 08**). March 17-18, 2008, Berlin, Germany.
Autori: Carlo Blundo, Giuseppe Persiano, Ahmad-Reza Sadeghi, Ivan Visconti.
- 28 Constant-Round Concurrent Non-Malleable Zero Knowledge in the Bare Public-Key Model.
In proceedings of the 35th International Colloquium on Automata, Languages and Programming (**ICALP 08**). July 6-13, 2008, Reykjavik - Iceland.
Lecture Notes in Computer Science, Vol. 5126, Pagg. 548-559, ISBN 3-540-7058201, 2008, Springer-Verlag, Heidelberg, Germania.
Autori: Rafail Ostrovsky, Giuseppe Persiano, Ivan Visconti.
- 29 Collusion-Free Protocols in the Mediated Model.
In proceedings of the Twenty-Eighth Annual IACR Crypto Conference (**CRYPTO 08**). August 17-21, 2008, Santa Barbara, USA.
Lecture Notes in Computer Science, Vol 5157, Pagg. 497-514, Springer-Verlag, Heidelberg,

- Germania, Agosto 2008, ISBN: 978-3-540-85173-8.
Autori: Joël Alwen, Abhi Shelat, Ivan Visconti.
- 30 Resetable and Non-Transferable Chip Authentication for E-Passports.
In proceedings of the 4th Workshop on RFID Security (**RFIDSec 08**). July 9-11, 2008, Budapest, Hungary.
Autori: Carlo Blundo, Giuseppe Persiano, Ahmad-Reza Sadeghi, Ivan Visconti.
- 31 Improved Security Notions and Protocols for Non-Transferable Identification.
In proceedings of 13th European Symposium on Research in Computer Security (**ESORICS 08**). October 6-8, 2008, Malaga, Spain.
Lecture Notes in Computer Science, Vol 5283, Pagg. 364-378, Springer-Verlag, Heidelberg, Germania, Ottobre 2008, ISBN: to appear.
Autori: Carlo Blundo, Giuseppe Persiano, Ahmad-Reza Sadeghi, Ivan Visconti.
- 32 User Privacy in Transport Systems Based on RFID E-Tickets.
In Workshop on Privacy in Location-Based Applications (**PILBA 2008**). October 9, 2008, Malaga, Spain.
CEUR Workshop Proceedings, to appear.
Autori: Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann.
- 33 Security Analysis of Italian E-Passports.
Third Italian Workshop on PRivacy and SEcurity (**PRISE 2008**), October 20, 2008, Rome, Italy.
Autori: Vincenzo Auletta, Carlo Blundo, Emiliano De Cristofaro, Giuseppe Persiano, Ivan Visconti.
- 34 Simulation-Based Concurrent Non-Malleable Commitments and Decommitments,
In proceedings of the 6th Theory of Cryptography Conference (**TCC 2009**). March 15-17 2009, San Francisco, CAL, USA.
Lecture Notes in Computer Science, Heidelberg, Germania.
Autori: Rafail Ostrovsky, Giuseppe Persiano, Ivan Visconti.
- 35 Co-Sound Zero-Knowledge with Public Keys,
In proceedings of the 2nd AFRICACRYPT Conference (**AFRICACRYPT 2009**). June 21-25 2009, Gammarath, Tunisia.
Lecture Notes in Computer Science, Heidelberg, Germania.
Autori: Carmine Ventre, Ivan Visconti.
- 36 Collusion-Free Multiparty Computation in the Mediated Model.
In proceedings of the Twenty-Nineth Annual IACR Crypto Conference (**CRYPTO 2009**). August 16-20, 2009, Santa Barbara, USA.
Lecture Notes in Computer Science, Springer-Verlag, Heidelberg, Germania, Agosto 2009.
Autori: Joël Alwen, Jonathan Katz, Yehuda Lindell, Giuseppe Persiano, Abhi Shelat and Ivan Visconti.

- 37 Semi-Destructive Privacy in RFID Systems.
In proceedings of the 5th Workshop on RFID Security (**RFIDSec 2009**). June 30 - July 2, 2009, Leuven, Belgium.
Autori: Paolo D'Arco, Alessandra Scafuro, Ivan Visconti.
- 38 Efficient RFID Security and Privacy with Anonymizers.
In proceedings of the 5th Workshop on RFID Security (**RFIDSec 2009**). June 30 - July 2, 2009, Leuven, Belgium.
Autori: Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann.
- 39 Revisiting DoS Attacks and Privacy in RFID-Enabled Networks.
In proceedings of the 5th International Workshop on Algorithmic Aspects of Wireless Sensor Networks (**ALGOSENSORS 2009**). July 10-11, 2009, Rhodes, Greece.
Autori: Paolo D'Arco, Alessandra Scafuro, Ivan Visconti.
- 40 Anonymizer-Enabled Security and Privacy for RFID.
In proceedings of the 8th Conference on CRYPTOLOGY AND NETWORK SECURITY (**CANS 2009**). December 12-14, Kanazawa, Japan.
Lecture Notes in Computer Science, Heidelberg, Germania.
Autori: Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann.
- 41 Efficiency Preserving Transformation for Concurrent Non-Malleable Zero Knowledge,
In proceedings of the 7th Theory of Cryptography Conference (**TCC 2010**). February 9-11 2010, Zurich, SWITZERLAND.
Lecture Notes in Computer Science, Heidelberg, Germania.
Autori: Rafail Ostrovsky, Omkant Pandey, Ivan Visconti.
- 42 Increasing Privacy Threats in the Cyberspace: the Case of Italian E-Passports,
In proceedings of the 1st International Workshop on Lightweight Cryptography for Resource-Constrained Devices (**WLC 2010**). January 2010, Tenerife, Canary Islands, SPAIN.
Lecture Notes in Computer Science, Heidelberg, Germania.
Autori: Vincenzo Auletta, Carlo Blundo, Angelo De Caro, Emiliano De Cristofaro, Giuseppe Persiano, Ivan Visconti.
- 43 Smart-Card Proxy Systems
In proceedings of the 4th Workshop in Information Security Theory and Practice (**WISTP 2010**): Security and Privacy of Pervasive Systems and Smart Devices. April 13-14 2010, Passau, GERMANY.
Lecture Notes in Computer Science, Heidelberg, Germania.
Autori: Giuseppe Cattaneo, Pompeo Faruolo, Vincenzo Palazzo, Ivan Visconti.
- 44 Statistically Binding Concurrent Non-Malleable Commitments and Decommitments.
In proceedings of the Workshop on Public-Key Cryptography (**PKC 2010**), May 26-28, 2010.

Lecture Notes in Computer Science, Springer-Verlag, 2010, Heidelberg, Germania.

Autori: Zhenfu Cao, Ivan Visconti, Zongyang Zhang.

45 PUF-Enhanced RFID Security and Privacy.

In Secure Component and System Identification (**SECSI 2010**). March 26-27, 2010, Cologne, Germany.

Autori: Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann.

46 On RFID Privacy with Mutual Authentication and Tag Corruption.

In proceedings of the 8th International Conference on Applied Cryptography and Network Security (**ACNS 2010**). June 22-25 2010, Beijing, China.

Lecture Notes in Computer Science, Heidelberg, Germania.

Autori: Frederik Armknecht, Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann.

47 Secure Set Intersection with Untrusted Hardware Tokens.

Topics in Cryptology (**CT-RSA 2011**). February 14-18 2011, San Francisco, USA.

Lecture Notes in Computer Science, Heidelberg, Germania.

Autori: Marc Fischlin, Benny Pinkas, Ahmad-Reza Sadeghi, Thomas Schneider, Ivan Visconti.

15.4 Capitoli di Libri

48 Location Privacy in RFID Enabled Applications.

Chapter of *Privacy in Location-Based Applications: Research Issues and Emerging Trends*.

Lecture Notes in Computer Science, Springer-Verlag, Heidelberg, Germania, Agosto 2009.

Autori: Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann.

49 Enhancing RFID Security and Privacy by Physically Unclonable Functions.

Chapter of *Towards Hardware Intrinsic Security: Foundation and Practice*.

Springer-Verlag, Heidelberg, Germania, 2010.

Autori: Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann.

50 A Distributed and Secure Architecture for Signature and Decryption Delegation Through Remote Smart Cards.

Chapter of *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions*.

IGI Global, Information Science Reference, 2011.

Autori: Giuseppe Cattaneo, Pompeo Faruolo, Ivan Visconti.

16 Attività Didattiche e Partecipazione a Scuole di Dottorato

16.1 Docenze per Studenti di Dottorato

- Settembre 2010: Ciclo di seminari su "Identification Protocols"

Ambito: ECRYPT PhD Summer School on Applied Cryptographic Protocols.

Luogo: Mykonos (Grecia).

- Novembre/Dicembre 2009: “Secure Cryptographic Protocols Against Man-in-the-Middle Attacks”
Ambito: corso offerto ai PhD student in computer science di UCLA, Los Angeles, USA.
Luogo: Los Angeles (USA).

16.2 Docenze per Studenti della Laurea

- Marzo - Giugno 2010: Corso di Recupero di Laboratorio di Sistemi Operativi (**36** ore)
Ambito: Corsi di Laurea in Informatica ed Informatica Applicata, anno accademico 2009/2010 (corso tenuto per carico didattico).
Luogo: Università di Salerno
- Marzo - Giugno 2009: Corso di Strumenti di Crittografia per la Sicurezza dell'Informazione (**48** ore)
Ambito: Corso di Laurea Specialistica in Informatica, anno accademico 2008/2009 (supplenza gratuita).
Luogo: Università di Salerno
- Marzo - Giugno 2009: Corso di Laboratorio di Sistemi Operativi (**64 + 24** ore)
Ambito: Corsi di Laurea in Informatica ed Informatica Applicata, anno accademico 2008/2009 (corso tenuto per carico didattico e supplenza).
Luogo: Università di Salerno
- Marzo - Giugno 2008: Corso di Strumenti di Crittografia per la Sicurezza dell'Informazione (**48** ore)
Ambito: Corso di Laurea Specialistica in Informatica, anno accademico 2007/2008 (supplenza gratuita)
Luogo: Università di Salerno
- Marzo - Giugno 2008: Corso di Laboratorio di Sistemi Operativi (**24** ore)
Ambito: Corsi di Laurea in Informatica ed Informatica Applicata, anno accademico 2007/2008 (corso tenuto per carico didattico e supplenza)
Luogo: Università di Salerno
- Ottobre - Dicembre 2007: Corso di Sicurezza su Reti (**48** ore)
Ambito: Corsi di Laurea in Informatica ed Informatica Applicata, anno accademico 2007/2008 (corso tenuto per carico didattico)
Luogo: Università di Salerno
- Marzo - Giugno 2007: Corso di Laboratorio di Crittografia e Sicurezza dell'Informazione (**64** ore)
Ambito: Corso di Laurea Specialistica in Informatica, anno accademico 2006/2007 (corso tenuto per carico didattico e supplenza gratuita)
Luogo: Università di Salerno

- Marzo - Giugno 2007: Corso di Laboratorio di Sistemi Operativi (**24** ore)
Ambito: Corsi di Laurea in Informatica ed Informatica Applicata, anno accademico 2006/2007
(corso tenuto per carico didattico)
Luogo: Università di Salerno
- Marzo - Giugno 2006: Laboratorio di Sistemi Operativi (**64 + 48** ore)
Ambito: Corsi di Laurea in Informatica ed Informatica Applicata, anno accademico 2005/2007
(corso tenuto per carico didattico ed incentivazione)
Luogo: Università di Salerno
- Gennaio 2006: SSL, TLS ed OpenSSL (seminario)
Ambito: Corso di sicurezza su reti tenuto dalla dott.ssa Masucci
Luogo: Università di Salerno
- Gennaio 2005: The TLS protocol (seminario)
Ambito: Corso di sicurezza su reti tenuto dalla dott.ssa Masucci
Luogo: Università di Salerno
- Giugno 2004: The OpenSSL package (seminario)
Ambito: Corso di sicurezza su reti tenuto dal prof. De Santis
Luogo: Università di Salerno
- Giugno 2004: The TLS protocol (seminario)
Ambito: Corso di sicurezza su reti tenuto dalla dott.ssa Masucci
Luogo: Università di Salerno
- Giugno 2003: The OpenSSL package (seminario)
Ambito: Corso di sicurezza su reti tenuto dal prof. De Santis
Luogo: Università di Salerno
- Giugno 2003: The TLS protocol (seminario)
Ambito: Corso di sicurezza su reti tenuto dalla dott.ssa Masucci
Luogo: Università di Salerno
- Marzo 2002: Network Security (corso di **16** ore)
Ambito: Master Universitario di secondo livello in Tecnologie del Software
Luogo: Ariano Irpino (AV) - Università del Sannio, Italia
- Aprile - Giugno 2001: Reti e Programmazione su Reti (corso di **50** ore - IFTS)
Ambito: Corso IFTS "Tecnico Esperto in Data Base distribuiti e sicurezza dati su reti"
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno
- Marzo - Giugno 2001: Word, Powerpoint e Reti (corso di **24** ore)
Ambito: Corso utile per il conseguimento della patente europea del computer
Luogo: Liceo Da Vinci, Salerno, Italia

- Maggio 2001: SSL and OpenSSL (Seminario)
Ambito: Corso di sicurezza su reti tenuto dal prof. De Santis
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno
- Aprile 2001: Network Security (corso di **16** ore)
Ambito: Master Universitario di secondo livello in Tecnologie del Software
Luogo: Ariano Irpino (AV) - Università del Sannio, Italia
- Gennaio 2001: Modules for Apache (Seminario)
Ambito: Corso di reti e programmazione su reti tenuto dal prof. Persiano
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno
- Gennaio 2001: OpenSSL (corso di **8** ore)
Ambito: Convenzione DIA - 3F Data Systems
Luogo: 3F Data Systems - Pozzuoli (Napoli), Italia
- Dicembre 2000: Corba (corso di **32** ore)
Ambito: Convenzione DIA - 3F Data Systems
Luogo: 3F Data Systems - Pozzuoli (Napoli), Italia
- Gennaio 2000: Modules for Apache (Seminario)
Ambito: Corso di reti e programmazione su reti tenuto dal prof. Persiano
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno

16.3 Tesi ed Altre Attività Didattiche

1. Attività di supervisione per il dottorato di ricerca in Informatica di Alessandra Scafuro, presso l'università di Salerno, per il periodo 1/11/2009–31/10/2012.
2. Attività di controrelatore per varie tesi di laurea e partecipazioni in varie commissioni di laurea dal 2005.
3. Partecipazione alle attività del programma ERASMUS, dal 2008.
4. Attività di relatore per 15 tesi di laurea relative alla laurea triennale in informatica, 1 tesi di laurea relativa alla laurea in informatica (vecchio ordinamento), 4 tesi di laurea relativa alla laurea specialistica in informatica.
5. Attività di tutoraggio per 15 tirocini.
6. Membro di commissioni giudicatrici per l'insegnamento di vari corsi universitari.
7. Cultore della materia per vari esami universitari.

16.4 Partecipazione a Corsi e Scuole

Ho partecipato ai seguenti corsi e scuole:

- *Titolo:* SecVote (summer school on e-voting)
Data: Settembre 2010
Luogo: Bertinoro, Forlì
- *Titolo:* Aeolus School on Security of Global Computers: Challenges and Approaches
Data: Ottobre 2007
Luogo: Salerno
- *Titolo:* ECRYPT School on Zero-Knowledge: Foundations and Applications
Data: Ottobre 2006
Luogo: Bertinoro, Forlì
- *Titolo:* Mathematical Aspects of Modern Cryptography
Data: Settembre 2005
Luogo: Bertinoro, Forlì
- *Titolo:* Introduction to the Wonderful World of Computational Complexity
Data: Aprile-Maggio 2005
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno
- *Titolo:* Topics in Cryptanalysis of Block Ciphers
Data: Maggio-Giugno 2004
Luogo: Département d'Informatique, École Normale Supérieure, Parigi, Francia
- *Titolo:* Error-Correcting Codes in Complexity Theory
Data: Maggio 2003
Luogo: Università "La Sapienza", Roma, Italia
- *Titolo:* Algorithms for selfish agents
Data: Maggio 2003
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno
- *Titolo:* Distributed Algorithms
Data: Marzo - Maggio 2003
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno
- *Titolo:* An Approach to the Verification of Concurrent Systems
Data: Ottobre 2002
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno
- *Titolo:* Concurrency Theory with Applications to Coordination and Security
Data: Giugno 2001
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno

- *Titolo:* Approximation and On-Line Algorithms
Data: Maggio 17-19, 2001
Luogo: University of Paris South - Orsay - Parigi - Francia
- *Titolo:* Fundamentals of Quantum Mechanics
Data: Settembre 11-15, 2000
Luogo: I.I.A.S.S. Vietri sul Mare, Salerno
- *Titolo:* Basics of Quantum Computing
Data: Settembre 11-15, 2000
Luogo: I.I.A.S.S. Vietri sul Mare, Salerno
- *Titolo:* Topics in Theoretical Computer Science: Complexity-based Cryptography, Randomness and Proof Systems
Data: Marzo 2000
Luogo: Dipartimento di Informatica ed Applicazioni - Università di Salerno

Autorizzazioni Legali

- Dichiaro, ai sensi del D.P.R 445/2000, che quanto riportato nel presente curriculum corrisponde a verità.
- Autorizzo, ai sensi del Dlgs 196 del 30 giugno 2003, il trattamento dei miei dati personali.

Ivan Visconti