

UNIVERSITÀ DEGLI STUDI DI MILANO

Procedura di selezione per la chiamata a professore di I fascia da ricoprire ai sensi dell'art. 18, comma 1, della Legge n. 240/2010 per il settore concorsuale 01/INFO-01 - INFORMATICA, settore scientifico-disciplinare INFO-01/A - Informatica presso il Dipartimento di Informatica "Giovanni Degli Antoni", Bando D.R. 7501/2024 del 05/12/2024 - Codice concorso 5653

## STELVIO CIMATO

### CURRICULUM VITÆ

#### Indice

<b>1</b>	<b>Informazioni Personali</b>	<b>2</b>
<b>2</b>	<b>Stato di servizio e formazione</b>	<b>2</b>
2.1	Posizione attuale . . . . .	2
2.2	Formazione . . . . .	2
2.3	Posizioni ricoperte . . . . .	2
<b>3</b>	<b>Attività didattica</b>	<b>3</b>
3.1	Insegnamenti per studenti di laurea triennale e magistrale . . . . .	3
<b>4</b>	<b>Attività di didattica integrativa e di servizio agli studenti</b>	<b>4</b>
4.1	Relatore di tesi di laurea . . . . .	4
4.2	Attività di servizio per corsi di dottorato . . . . .	4
4.3	Lezioni e Attività per Corsi di Formazione, Perfezionamento e Corsi Post-Laurea . .	6
<b>5</b>	<b>Attività di ricerca e pubblicazioni scientifiche</b>	<b>7</b>
5.1	Attività per progetti di ricerca . . . . .	7
5.2	Brevetti . . . . .	9
5.3	Attività di organizzazione e di valutazione . . . . .	9
5.4	Partecipazione in qualità di relatore a congressi e convegni di interesse internazionale	13
5.5	Pubblicazioni . . . . .	16
<b>6</b>	<b>Attività istituzionali, organizzative, di servizio, e di terza missione</b>	<b>29</b>
6.1	Attività istituzionali . . . . .	29
6.2	Attività di servizio per il Dipartimento e il Collegio Didattico . . . . .	29
6.3	Attività di Terza Missione . . . . .	30

# 1 Informazioni Personali

**Nome:** Stelvio

**Cognome:** Cimato

**Indirizzo:** Dipartimento di Informatica  
Università degli Studi di Milano  
Via Celoria, 18  
20133 Milano

**Telefono** +39-02-50316258

**E-mail:** stelvio.cimato@unimi.it

**URL:** <http://www.di.unimi.it/cimato>

## 2 Stato di servizio e formazione

### 2.1 Posizione attuale

Dal 1 Aprile 2016 è in servizio come Professore Associato S.S.D. INF/01 presso il Dipartimento di Informatica dell'Università degli Studi di Milano.

### 2.2 Formazione

*Febbraio 2023* - Ha conseguito l'Abilitazione scientifica nazionale a Professore di I Fascia (I Fascia - ASN 2021-2023) per il settore concorsuale (01/B1) Informatica

*Gennaio 2014* - Ha conseguito l'Abilitazione scientifica nazionale a Professore di II Fascia per il settore concorsuale (01/B1) Informatica

*Febbraio 1999* Ha conseguito il titolo di Dottore di Ricerca in Informatica (X ciclo - 4 anni), presso il Dipartimento di Scienze dell'Informazione dell'Università di Bologna in consorzio con le Università di Padova e Venezia, supervisore prof. P. Ciancarini

*Giugno 1994* Laurea in Scienze dell'Informazione conseguita presso l'Università degli Studi di Salerno. Voto di Laurea: 110/110 e lode.

### 2.3 Posizioni ricoperte

*Gennaio 2005- Marzo 2016* In servizio come Ricercatore Confermato presso l'Università degli Studi di Milano.

*Febbraio 2004 - Dicembre 2004* è stato titolare di un Assegno di Ricerca biennale presso il Dipartimento di Informatica e Applicazioni dell'Università di Salerno per il progetto "Protocolli Crittografici per Servizi Internet", sotto la supervisione del Prof. Carlo Blundo.

*Settembre 1999 - Dicembre 2003* è stato Titolare di un Assegno di Ricerca biennale, rinnovato ed esteso per ulteriori due anni, presso il Dipartimento di Informatica e Applicazioni dell'Università di Salerno, nell'ambito del progetto "Schemi di Identificazione" sotto la supervisione del Prof. Alfredo De Santis.

*Novembre 1994- Novembre 1998* Frequenta il Corso di Dottorato di Ricerca in Informatica (X ciclo), presso il Dipartimento di Scienze dell'Informazione dell'Università di Bologna in consorzio con le Università di Padova e Venezia.

### **3 Attività didattica**

#### **3.1 Insegnamenti per studenti di laurea triennale e magistrale**

Ha tenuto i seguenti corsi per il Corso di Laurea Magistrale in Sicurezza Informatica, Corso di Laurea Magistrale in Scienze e Tecnologie dell'Informazione/Informatica, e per il corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche presso la Università di degli Studi di Milano.

- Anni Accademici: 2022/23, 2023/24, 2024/25
  - Docente del “Corso di Sicurezza dei sistemi e delle reti informatiche” (4 cfu – 32 ore)
    - Corso di Laurea Magistrale in Sicurezza Informatica, mutuato per corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Sicurezza delle reti 2” (6 cfu – 48 ore) - Corso di Laurea Magistrale in Sicurezza Informatica
  - Docente del “Corso di Crittografia” (6 cfu – 48 ore) Corso di Laurea Magistrale in Sicurezza Informatica, mutuato per corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Crittografia (Edizione ONLINE)” (6 cfu) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Sicurezza dei sistemi e delle reti informatiche (Edizione ONLINE)” (6 cfu) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
- Anni Accademici: 2016/2017, 2017/18, 2018/19, 2019/20, 2020/21, 2021/22
  - Docente del “Corso di Sicurezza dei sistemi e delle reti informatiche” (10 cfu – 80 ore) Corso di Laurea Magistrale in Sicurezza Informatica, mutuato per corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Crittografia” (6 cfu – 48 ore) Corso di Laurea Magistrale in Sicurezza Informatica, mutuato per corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Crittografia (Edizione ONLINE)” (6 cfu) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Sicurezza dei sistemi e delle reti informatiche (Edizione ONLINE)” (12 cfu) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
- Anni Accademici: 2014/2015, 2015/2016
  - Docente del “Corso di Crittografia” (6 cfu – 48 ore) Corso di Laurea Magistrale in Sicurezza Informatica, mutuato per corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Crittografia (Edizione ONLINE)” (6 cfu) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Advanced Computer Programming (in Inglese)” (2 cfu – 16 ) Corso di Laurea Magistrale in Scienze e Tecnologie dell'Informazione/Informatica
- Anni Accademici: 2009/2010, 2010/2011, 2011/2012, 2012/2013, 2013/2014

- Docente del “Corso di Crittografia” (6 cfu – 48 ore) Corso di Laurea Magistrale in Sicurezza Informatica, mutuato per corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
- Docente del “Corso di Crittografia (Edizione ONLINE)” (6 cfu) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
- Anni Accademici: 2005/2006, 2006/2007, 2007/2008, 2008/2009
  - Docente del “Corso di Crittografia” (6 cfu – 48 ore) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Crittografia (Edizione ONLINE)” (6 cfu) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
  - Docente del “Corso di Laboratorio di Crittografia Applicata” (6 cfu – 48 ore) corso triennale in Sicurezza dei Sistemi e delle Reti Informatiche
- Anno Accademico 2004/2005
  - Docente del “Corso di Crittografia” (6 cfu – 48 ore)
  - Cicli di seminari tenuti per l’insegnamento di “Sicurezza su reti”, Corso di Laurea in Informatica, Facoltà di Scienze Matematiche, Fisiche e Naturali, Università di Salerno, anni accademici 1999/2000, 2000/2001, 2001/2002, 2002/2003, 2003/2004.
  - Cicli di seminari tenuti per l’insegnamento di “Tecnologie di Sviluppo per il Web”, Corso di Laurea in Informatica, Facoltà di Scienze Matematiche, Fisiche e Naturali, Università di Salerno, anno accademico 2002/2003.
  - Cicli di seminari tenuti per l’insegnamento di “Informatica Generale”, Corso di Laurea in Scienze delle Comunicazioni, Facoltà di Lettere e Filosofia, Università di Bologna, anno accademico 1998/99.
  - Cicli di seminari tenuti per l’insegnamento di “Ingegneria del Software”, Corso di Laurea in Informatica, Facoltà di Scienze, Università di Bologna, anni accademici 1995/96, 1996/97 e 1997/98.

## 4 Attività di didattica integrativa e di servizio agli studenti

### 4.1 Relatore di tesi di laurea

Ha svolto attività di supervisione in qualità di relatore per di Tesi di Laurea per l’Università degli Studi di Milano, per più di circa **130** studenti: in particolare è stato relatore per circa **50** studenti del corso di Laurea Magistrale in Sicurezza Informatica; è stato relatore per circa **70** studenti del corso di Laurea triennale in Sicurezza dei Sistemi e delle Reti Informatiche; è stato relatore inoltre per studenti del corso di laurea magistrale in Informatica e per il corso di Scienze e Tecnologie dell’Informazione e per il corso triennale in Comunicazione Digitale presso il Dipartimento di Informatica dell’Università degli Studi di Milano.

### 4.2 Attività di servizio per corsi di dottorato

- Dal 2022 è membro del Collegio dei Docenti della Scuola di Dottorato Nazionale in Blockchain e Distributed Ledger Technologies dell’Università degli Studi di Camerino.
- 2011-2018 è membro del Collegio dei Docenti della Scuola di Dottorato in Informatica dell’Università degli Studi di Milano.

- Dal 2010 è membro coordinatore del collegio di dottorato in “Multimedia, Distributed and Pervasive Systems”, nell’ambito della collaborazione con Chair of Distributed Information Systems of the Faculty of Informatics and Mathematics of the University of Passau e con INSA - University of Lyon.

#### **4.2.1 Relatore di tesi di dottorato**

È /è stato supervisore e relatore dei seguenti studenti che hanno frequentato/frequentano attualmente la scuola di dottorato in Informatica:

- XXXIX Ciclo, candidato Taha Ramzan, Dottorato intersettoriale Università degli studi di Milano
- XXXIX Ciclo, candidato Jahan Zeb Shahid, Dottorato nazionale in Blockchain and Distributed Ledger Technologies, Università degli studi di Camerino
- XXXIV Ciclo candidata Maria Chiara Molteni, Dottorato di Ricerca in Informatica dell’Università degli Studi di Milano, dottorato conseguito con tesi dal titolo “On the security of cryptographic circuits: protection against probing attacks and performance improvement of garbled circuits”.
- XXIX Ciclo, candidata Silvia Mella, dottorato conseguito con tesi dal titolo “Analysis of cryptographic algorithms against theoretical and implementation attacks”, Dottorato di Ricerca in Informatica dell’Università degli Studi di Milano.

È/è stato co-supervisore e correlatore della tesi di dottorato in Informatica dell’Università degli Studi di Milano per i seguenti studenti:

- XXX Ciclo, candidato Maryam Ehsanpour, dottorato conseguito con tesi dal titolo “Toward Lower Communication in Garbled Circuit Evaluation”
- XXV Ciclo, candidato Maryam Sepehri, dottorato conseguito con tesi dal titolo “Privacy-preserving Query Processing over Outsourced Encrypted Data and Multi-Party Computation”
- XXIV Ciclo, candidato Francesco Pagano, dottorato conseguito con tesi dal titolo “A Distributed Approach to Privacy on the Cloud”

#### **4.2.2 Membro di commissioni di dottorato nazionali ed internazionali**

- Nel Marzo 2019 è stato membro della commissione per l’esame finale di dottorato Informatica 31° ciclo, Università Ca’ Foscari Venezia
- Nel Settembre 2012 è stato membro della commissione giudicatrice per il Ph.D dello studente Jacques Machizaud presso Université Jean Monnet, Saint Etienne, France (“Cryptographie Visuelle pour l’authentification de documents”, relatore prof. Thierry Fournel)
- Nel 2013 è stato nominato componente supplente nella commissione giudicatrice per il conseguimento del titolo di Dottore in Ricerca in Informatica – XI Ciclo dell’Università degli studi di Salerno (Coord. del dottorato Prof. G. Persiano)
- Nel 2009 è stato nominato componente supplente nella commissione giudicatrice per il conseguimento del titolo di Dottore in Ricerca in Informatica – VII Ciclo dell’Università degli studi di Salerno (Coord. del dottorato Prof. M. Napoli)
- Nel 2008 è stato nominato componente supplente nella commissione giudicatrice per il conseguimento del titolo di Dottore in Ricerca in Informatica – VI Ciclo dell’Università degli studi di Salerno (Coord. del dottorato Prof. M. Napoli)

#### 4.2.3 Attività didattica per il dottorato di ricerca

E' stato titolare dei seguenti insegnamenti per il dottorato di ricerca in Informatica presso Università degli studi di Milano

- A.A. 2020/2021, Introduction to quantum information and cryptography (Dottorato in informatica) 2cfu, 5 ore.
- A.A. 2022/2023, Introduction to quantum information and cryptography (Dottorato in informatica) 2cfu, 5 ore.
- A.A. 2024/2025, Introduction to quantum information and cryptography (Dottorato in informatica) 2cfu, 5 ore.

#### 4.2.4 Seminari e didattica per Corsi di Laurea Internazionali

- Gennaio 2025 Ciclo di seminari su "Introduction to Quantum Information and Cryptography" (4 ore) presso INSA Lione
- Gennaio 2024 Ciclo di seminari su "Introduction to Quantum Information and Cryptography" (4 ore) presso INSA Lione

#### 4.3 Lezioni e Attività per Corsi di Formazione, Perfezionamento e Corsi Post-Laurea

- Dal 2022 al 2024 Docente del modulo di "Web and Mobile Security" per il Master in Cybersecurity organizzato dall'Università degli studi di Milano (20 ore)
- Dal 2018 al 2021 Docente del modulo di "System and Network Security" per il Master in Cybersecurity organizzato dall'Università degli studi di Milano (20 ore)
- Docente del modulo di "Sicurezza", 40 ore, per il Corso ITS "Digitalizzazione dei processi industriali", per la Fondazione ITS per le Nuove tecnologie per il Made in Italy, 2024
- Docente del modulo di "Informatica", 20 ore, per il Corso ITS "Tecnico Superiore per l'automazione ed i sistemi mecatronici - Automazione e innovazione per la transizione ecologica", per la Fondazione ITS per le Nuove tecnologie per il Made in Italy, 2024
- Docente del modulo di "Informatica", 20 ore, per il Corso ITS "Tecnico Superiore per l'automazione ed i sistemi mecatronici - Automazione e innovazione per la transizione ecologica", per la Fondazione ITS per le Nuove tecnologie per il Made in Italy, 2023
- Docente del modulo di "Informatica", 20 ore, per il Corso IFTS "Digital Automation in Manufacturing 4.0", per la Fondazione ITS per le Nuove tecnologie per il Made in Italy, 2022
- Docente del modulo di "Informatica", 10 ore, per il Corso IFTS "Digital Automation in Manufacturing 4.0", per la Fondazione Istituto Tecnico Superiore Efficienza Energetica, Maggio 2021
- Docente del modulo di "Sicurezza", 5 ore, per il Corso ITS "Tecnico Superiore per il Risparmio Energetico nell'Edilizia Sostenibile", per la Fondazione Istituto Tecnico Superiore Efficienza Energetica, Dicembre 2014
- Docente del modulo di "Sicurezza", 10 ore, per il corso IFTS *Tecnico superiore per la comunicazione ed il multimedia* in collaborazione con l'Istituto Tecnico C.P.A.C.L.E. "L. Pacioli" di Crema, Marzo 2006.

- Docente del modulo di “Realizzazione di pagine web statiche”, 20 ore, per il corso IFTS *Tecnico superiore per la comunicazione ed il multimedia* in collaborazione con l’Istituto Tecnico C.P.A.C.L.E. “L. Pacioli” di Crema, Marzo 2006.
- Docente del modulo di “Photoshop”, 20 ore, per il corso IFTS *Tecnico superiore per la comunicazione ed il multimedia* in collaborazione con l’Istituto Tecnico C.P.A.C.L.E. “L. Pacioli” di Crema, Marzo 2006.

## 5 Attività di ricerca e pubblicazioni scientifiche

L’attività di ricerca si svolge nell’ambito della crittografia e della sicurezza dati, interessandosi a tematiche legate alla protezione della privacy e dei dati personali, con sviluppo e applicazione di tecniche e protocolli su diversi aspetti di ricerca, tra i quali la crittografia visuale, la computazione sicura su cloud, la biometria e il controllo degli accessi. Seguendo tali tematiche è/è stato coinvolto in progetti di ricerca nazionali ed internazionali ed ha pubblicato diversi articoli in riviste e conferenze internazionali.

### 5.1 Attività per progetti di ricerca

È/è stato coinvolto in unità di ricerca i cui progetti sono stati approvati e finanziati, partecipando attivamente alle attività di ricerca, alla stesura dei report ed ai meeting di progetto.

#### 5.1.1 Progetti Europei

- Project 101126524 Erasmus+ Programme (ERASMUS+): Chair Jean Monnet The Future of Money and Finance: between Blockchain, Sustainability, and the Law (FutMoFin) Resp. prof. Giulio Peroni, Dip di Diritto pubblico italiano e sovranazionale
- Erasmus+ Erasmus Mundus Design Measures – (ERASMUS-EDU-2022-EMJM-DESIGN) CALL ID: ERAS MUS-EDU-2022-PEX-EMJM-MOB - Master in Intelligent Systems for a Sustainable Digital Transformation of the Society MINDS. Role: Responsabile for UNIMI
- SMART-BEAR
- TENACIOUS: Trustworthy sEmaNtic Aware marketplaCe for Interoperable cLOUd Services, selected for the first phase of the European project funded by the European Commission under the European Union’s Horizon 2020 Research and Innovation Programme (Call topic ICT-54) and part of the European Commission’s Next Generation Internet (NGI) initiative. Role: co-leader together with E. Bellini, B. Di Martino, A. Esposito, and E. Damiani
- European Project H2020 THREAT-ARREST (Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training) (2018-21), Grant Number 786890, Responsabile scientifico UNIMI: prof. Ernesto Damiani, Role: WP-Leader(36 mesi)
- European Project Erasmus+ FIT EUROPE (Future IT leaders for a multicultural, digital Europe) 9/2019-8/2022 Référence : 2019-1-FR01-KA203-063041. Responsabile scientifico UNIMI: prof. Ernesto Damiani, (36 mesi)
- European Project H2020-MSCA-RISE-2019 AERAS (A CybEr range tRaining platform for medicAl organisations and systems Security). Responsabile scientifico UNIMI: prof. Ernesto Damiani,

- COST Action CA17124 - Digital forensics: evidence analysis via intelligent systems and practices, Proposal Reference OC-2017-1-22305, Chair Jesus Medina Moreno Università di Cadice, vice Chair prof. Stefania Costantini - Univ. dell'Aquila -Start action 10/09/2018 End of Action - 09/09/2022 Role: Responsabile per il nodo di Univ. degli studi di Milano.
- European Project H2020 TOREADOR - Trustworthy model-aware Analytics Data platform Grant Number 688797 (2015-18), Responsabile scientifico UNIMI: prof. Ernesto Damiani, (36 mesi)
- European Project FP7: PRACTICE (PRivacy-preserving CompuTation In The Cloud) FP7-609611 (2013-16), Responsabile scientifico UNIMI: prof. Ernesto Damiani, Role: WP-Leader (36 mesi)
- European Project FP7: CUMULUS - Certification infrastructure for Multi-Layer cloud Services FP7-318580 (2012-2015), Responsabile scientifico UNIMI: prof. Ernesto Damiani, (36 mesi)
- European Project FP7: ASSERT4SOA (Advanced Security Service cERTificate for SOA) FP7-257351 (2010-2013), Responsabile scientifico UNIMI: prof. Ernesto Damiani, (36 mesi)
- European Project FP7: SECURESCM (SECURE Supply Chain Management) FP7- 213531 (2008-2011) , Responsabile scientifico UNIMI: prof. Ernesto Damiani, Role: WP-Leader (36 mesi)

### 5.1.2 Progetti Nazionali

- PRIN 2022: SAFEST: " Trust assurance of Digital Twins for medical cyber-physical systems" resp. scientifico prof. A. Gargantini Univ di Bergamo, Unità di ricerca di Milano, resp. prof. E. Riccobene. CUP: G53O23002770006
- bando PNRR Next Generation Healthcare Center – NGHC, progetto presentato dal Politecnico di Milano, in collaborazione con la Statale per la concessione di finanziamenti destinati alla realizzazione o ammodernamento di Infrastrutture tecnologiche di innovazione
- PRIN 2008: PEPPER: Privacy E Protezione di dati PERSONALI, Responsabile Prof. S. Paraboschi, Unità di ricerca di Milano, resp. scientifico Prof. P. Samarati. (24 mesi)
- PRIN 2006: Basi di dati crittografate, Responsabile Prof. S. Paraboschi, Unità di ricerca di Milano, resp. scientifico Prof. P. Samarati. (24 mesi)
- PRIN 2002 *Metodi Formali per la Sicurezza e il Tempo (MEFISTO)*, resp. scientifico
- PRIN 2010 GenData 2020 (Data-Centric Genomic Computing) (PRIN 2010) Responsabile Prof. S. Ceri, Unità di ricerca di Milano, resp. prof. P. Samarati (36 mesi)  
Prof. R. Gorrieri, Unità di ricerca di Salerno, resp. scientifico Margherita Napoli (24 mesi)
- Progetto *Pubblicità Online: Nuove Misure per Nuovi Media. Auditing e Accounting Sicuro sul Web*, nell'ambito del programma CNR-Agenzia 2000. (12 mesi)
- Progetto MURST 40%: "Metodologie e Strumenti di Verifica e Valutazione di Funzionalità, Prestazioni e Affidabilità di Processi e Prodotti nell'Ingegneria del Software", 1995

### 5.1.3 Progetti Locali

È stato Coordinatore e Responsabile dei seguenti progetti:



- Progetto interdipartimentale SEED 2019: CRIPTO S.O.S Criptovalute: sfida alla sovranità statale? Un'indagine storico-economica, giuridica e tecnica. PI: Martino Zulbert, Dipartimento di Diritto Pubblico Italiano e Sovranazionale. Ruolo: Capo Unità Dipartimentale (CUD) 5/2020-5/2021
- Nel 2012-2013 ha coordinato le attività relative al progetto “Laboratorio Itinerante per bambini: nuove tecnologie per superare le barriere”, assegnato (10.000€) nell’ambito del Bando regione Lombardia volontariato 2012-13, presentato dall’Associazione Amici del Montessori, Comune di Crema, e Dip. di Informatica dell’Università degli Studi di Milano. Nell’ambito di tale progetto ha organizzato e tenuto un Ciclo di lezioni di “Introduzione alla didattica con l’Ipad”
- Coordinatore e Responsabile del progetto *Protocolli di Autenticazione per Smartcard e Applicazioni a Mobile Commerce*, finanziato dalla Università di Salerno, nell’ambito delle iniziative condotte da giovani ricercatori - Anno 2001. (12 mesi)
- Coordinatore e Responsabile del progetto *Nuove Tendenze nel Commercio Elettronico e Pubblicità Online: gli E-Coupon*, finanziato dalla Università di Salerno nell’ambito delle iniziative condotte da giovani ricercatori - Anno 2000. (12 mesi)

## 5.2 Brevetti

Coinventore dei seguenti brevetti:

- Cimato S., Gamassi M., Piuri V., Sana D., Sassi R., Scotti F. “*Method for generating and verifying security information obtained by means of biometric readings*”, European patent no. WO2007113888, October, 2007
- Cimato S., Gamassi M., Piuri V., Sana D., Sassi R., Scotti F. “*Metodo di generazione e di verifica di una informazione di sicurezza ottenuta mediante letture biometriche* N. MI2006A000641. Università degli Studi di Milano. Domanda di brevetto depositata il 31 Marzo 2006.

## 5.3 Attività di organizzazione e di valutazione

### 5.3.1 Editorial Board di Riviste

- Da aprile 2024 è membro dell’editorial board della rivista internazionale *Journal of Surveillance, Security and Safety (JSSS)*, OAE publishing
- Da Gennaio 2024 è associate editor della rivista internazionale *Journal of Electronic Imaging (JEI)*, SPIE, ISSN:1017-9909E-ISSN:1560-229X (indicizzata Scopus)
- Da maggio 2019 è membro dell’editorial board della rivista internazionale *Future Internet*, MDPI Publisher, ISSN 1999-5903, (indicizzata Scopus)
- Da giugno 2018 è membro dell’editorial board della rivista internazionale *Cryptography*, MDPI Publisher, ISSN: 2410-387X (indicizzata Scopus)
- Da marzo 2018 fino a Dicembre 2024 è membro dell’editorial board della rivista internazionale *Security and Communication Networks*, Hindawi (indicizzata Scopus)
- Da gennaio 2017 fino a Dicembre 2020 è membro dell’editorial board della rivista internazionale *Electronic Commerce Research and Applications*, Elsevier (indicizzata Scopus)
- Da gennaio 2008 a gennaio 2013 è membro dell’ editorial board della rivista internazionale *Recent Patents on Computer Science*, Bentham Science Publishers
- Ha fatto parte dell’ IEB per lo Special Issue of Information Systems Frontiers on Intelligent Systems and Smart Homes, pubblicato da Springer (2007)

### 5.3.2 Attività organizzative per Convegni Scientifici

- Organizzatore e program chair del workshop *Permutation-based Crypto 2025* May 4, 2025 - Madrid, Spain co-located with EUROCRYPT 2025 (con Joan Daemen, Silvia Mella, e Gilles van Assche)
- Program Chair *COMPSAC 2025: The 49th IEEE Computer Society International Conference on Computers, Software & Applications* Toronto, Canada- July 8-11, 2025
- Program Chair *ICSEB 2022, 6th International Conference on Software and e-Business*, Shenzhen, China - December 09-11, 2022
- Program Chair *ICSEB 2021, 5th International Conference on Software and e-Business* , virtual — December 3-5, 2021
- Program Chair *ICSEB 2020, 4th International Conference on Software and e-Business* , virtual — December 18-20, 2020
- Program Chair *COMPSAC 2019: The 43rd IEEE Computer Society International Conference on Computers, Software & Applications* Milwaukee, USA - July 15-19, 2019
- Technical Committee Chair, *ICSEB 2019 3rd International Conference on Software and e-Business*, Tokyo, Japan, December 9-11, 2019
- Organizzatore e program chair del workshop *Advances in Permutation Based Cryptography*, October 10, Milan, Italy, 2018.
- Organizzatore del 20th workshop del collegio di dottorato MDPS-IRIXYS in “Multimedia, Distributed and Pervasive Systems” June 24-29, Gargnano, Italy, 2018.
- Program Chair *COMPSAC 2018: The 42nd IEEE Computer Society International Conference on Computers, Software & Applications* Tokyo, Japan - July 23-27, 2018
- Workshop Chair *COMPSAC 2017: The 41th IEEE Computer Society International Conference on Computers, Software & Applications* Turin, Italy - July 3-8, 2017
- Workshop Co-Chair *COMPSAC 2016: The 40th IEEE Computer Society International Conference on Computers, Software & Applications* Atlanta, Georgia, USA - June 10-14, 2016
- Organizzatore del 16th workshop del collegio di dottorato MDPS in “Multimedia, Distributed and Pervasive Systems” June 19-25, Gargnano, Italy, 2016.
- Fast Abstract Co-Chair *COMPSAC 2015: The 39th IEEE Computer Society International Conference on Computers, Software & Applications* Taichung, Taiwan - July 1-5, 2015
- Dal 2009 al 2025 Organizzatore e Program Chair del Workshop *SAPSE 2025 - International Workshop on Security Aspects of Process and Services Engineering* in conjunction with COMPSAC
- Organizzatore del 6th workshop del collegio di dottorato MDPS in “Multimedia, Distributed and Pervasive Systems” June 20-24, Crema, Italy, 2011.
- General Chair della conferenza *4th Conference on Security in Communication Networks (SCN'04)*, Amalfi, Italia, Settembre 2004.
- Publication Chair della conferenza *23rd International Information Security Conference (SEC 2008)* Milano, Italia, Settembre 2008.
- Membro del comitato organizzatore della conferenza *17th International Conference on Distributed Computing (DISC'03)*, Sorrento, Italia, Ottobre 2003.
- Membro del comitato organizzatore della conferenza *Security in Communication Network (SCN'02)*, Amalfi, Italia, Settembre 2002.

### 5.3.3 Comitati di Programma per Convegni Scientifici

Membro del comitato di programma delle seguenti conferenze/workshop internazionali

- SEKE -International Conference on Software Engineering and Knowledge Engineering (2011-2025)
- ICME - IEEE International Conference on Multimedia and Expo (2011-2025)
- ICSEB - International Conference on Software and e-Business, (2017-2024)
- ICISSP - International Conference on Information Systems Security and Privacy (2015-2025)
- IDEAL - International Conference on Intelligent Data Engineering and Automated Learning, (2010-2024)
- ICCSIT - International Conference on Computer Science and Information Technology (2018-2020)
- ICISA - iCatse Conference on Information Science and Applications (2016- 2019)
- PSBD - 4th International Workshop on Privacy and Security of Big Data (2017)
- KES - International Conference on Knowledge-Based and Intelligent Information and Engineering Systems (2017-20)
- SIN - International Conference on Security of Information and Networks (2015-2020)
- AICCSA 2020 - ACS/IEEE International Conference on Computer Systems and Applications, Antalya, Turkey - November 2-5, 2020
- DLT - Distributed Ledger Technology Workshop, (2018-2025)
- MLWCOM 2019 - International Workshop on Machine Learning for Wireless Communications -, Barcelona, Spain, June 29- July 3rd, 2019
- WCNC-SFCS 2019 - IEEE Wireless Communications and Networking Conference, Marrakech, Morocco, 15-18 April, 2019
- ISIC - International Conference on Information Security and Intelligent Computing at Shennongjia, Hubei (2017)
- ICIT - 16th International Conference on Information Technology, Bhubaneswar, India December 21-23, 2017
- SAPSE - IEEE International Workshop on Security Aspects of Process and Services Engineering in conjunction with COMPSAC IEEE conference (2009- 2020)
- ESAS - IEEE International Workshop on E-Health Systems and Semantic Web (2016-2020)
- SFCS - IEEE International Workshop on Security and Forensics in Communication Systems in conjunction with AsiaCCS (2014-15)
- ICB - International Conference on Biometrics (2015)
- WPS - 5th FTRA International Workshop on Web and Pervasive Security, Jeju, Korea (2012)
- SETOP - 5th SETOP International Workshop on Autonomous and Spontaneous Security, Pisa, Italy (2012)
- NPC - 9th IFIP International Conference on Network and Parallel Computing, Gwangju, Korea (2012)
- ISPEC - International Conference on Information Security Practice and Experience (2014)
- POLICE - International Workshop on Security Policies in Cloud Environment (2013- 14)

- CIS - International Conference on Computational Intelligence and Security (2005-2018)
- NSS - IFIP International Workshop on Network and System Security (2007-2011)
- ICSNC - International Conference on Systems and Networks Communications, (2008-2017)
- ISSA - Annual Information Security South Africa Conference (2005-2012)
- SECURWARE - International Conference on Emerging Security Information, Systems and Technologies, (2011-2014)
- IMMM - International Conference on Advances in Information Mining and Management (2011-2012)
- SESYS - Security Systems track of the International Conference on Systems and Networks Communications (2006-2007)
- SECRIPT - International Conference on Security and Cryptography, Milan, Italy, (2009)
- BPS - 1st International Workshop on Business Processes Security, in conjunction with DEXA 2009, Linz, Austria, (2009)
- ICICS - Ninth International Conference on Information and Communications Security, Zhengzhou, Henan, China, (2007)
- IS - International Symposium on Information Security, (2006-2007)
- WISH - International Workshop on Intelligent Systems and Smart Home, (2007-2008)
- ASIACCS - ACM Symposium on Information, Computer and Communications Security, Singapore (2007)

#### **5.3.4 Altre Attività di organizzazione e di ricerca**

- Dal 2012 al 2015 è stato responsabile e coordinatore del Laboratorio di Ricerca in Crittografia e Computazione Sicure (CR&SCO-Cryptography and Secure Computation Laboratory) presso il Dipartimento di Informatica dell'Università degli Studi di Milano, Dal 2016 le attività del laboratorio sono state assorbite dal SESAR-Lab coordinato dal prof. Ernesto Damiani presso il Dipartimento di Informatica dell'Università degli studi di Milano, di cui attualmente è membro.
- Da Gennaio 2008 ad Aprile 2010 è stato co-fondatore e responsabile scientifico per SENSURE, spin-off creato dalla Università degli Studi di Milano (Dipartimento di Tecnologie dell'Informazione) e dal Politecnico di Milano (Dipartimento di Elettronica e Informazione)
- Dal 26 giugno 2017 è stato nominato senior member per IEEE (Institute of Electrical and Electronics Engineers).

#### **5.3.5 Attività di valutazione**

Revisore per la Valutazione di progetti per conto del Ministero dell'Istruzione, dell'Università e della Ricerca e/o di Università nazionali

- Valutatore per progetti di ricerca per il programma "Computer Science Discovery Grant application", Natural Sciences and Engineering Research Council of Canada (NSERC), Canada (2019, 2020)
- Valutatore di Progetti di Ricerca per l'iniziativa Research for Innovation - REFIN, Regione Puglia, 2019

- Valutatore per una proposta di progetto presentata nell'ambito del Bando di Ateneo Joint Projects 2016 promosso dall'Università di Verona.
- Valutatore per progetti di ricerca per il programma SIR (Scientific Independence of young Researchers) 2014", Ministero dell'Istruzione, dell'Università e della Ricerca, Italia
- In dicembre 2024, ha partecipato, in qualità di membro, a una commissione di selezione per bandi di concorso per personale di categoria D, Università degli Studi di Milano Bicocca
- Ha partecipato, come membro, in una commissione di selezione per un bando di concorso per ricercatore RTD-A, Università Ca' Foscari di Venezia, settembre 2018
- Dal 2015 È iscritto all'albo dei revisori (REPRISE) del MIUR Ministero dell'Istruzione, dell'Università e della Ricerca
- Ha partecipato, in qualità di membro, a diverse commissioni di selezione per bandi di concorso per assegni di ricerca, per personale di categoria D ed EP, Università degli Studi di Milano
- Valutatore per procedure competitive per l'assegnazione dei fondi di Ateneo destinati all'attivazione di assegni di ricerca per conto dell'Università di Verona.
- Valutatore di 2 Progetti SIR (Scientific Independence of young Researchers) 2014

### 5.3.6 Attività di Revisione

Ha svolto attività di revisione per diverse riviste, tra le quali:

- IEEE Transaction on Information Theory, IEEE Transaction on Knowledge and Data Engineering, IEEE Transaction on Information Forensics and Security, IEEE Transaction on Parallel and Distributed Systems, IEEE Transaction on Image Processing, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transaction on Multimedia, IEEE Internet Computing, IEEE Computers Journal of Information Security and Applications, Theoretical Computer Science, ACM Transaction on Web, Electronic Commerce Research and Applications, Computer Networks (Elsevier) Transactions on Data Hiding and Multimedia Security (Springer) Computers & Security, MultimediaTools and Applications (Elsevier) Multimedia Systems Springer Journal of Systems and Software (Elsevier) Journal of Computer Security (IOS Press) Journal of Visual Communication and Image Representation Design, Codes and Cryptography (Kluwer) Imaging Science Journal (Maney Publishing) Eurasip Journal on Information Security, Journal of Computer and Science Technology (Springer) Image and Vision Computing (Elsevier) Information Sciences (Elsevier) Security and Communication Networks (Springer) Optical Engineering (SPIE) Signal Image and Video Processing Telecommunication Systems (Springer)

## 5.4 Partecipazione in qualità di relatore a congressi e convegni di interesse internazionale

### 5.4.1 Seminari su Invito

- Keynote speaker *Secure Data Sharing and Mining on the Cloud*, 2nd International Conference on Security with Intelligent Computing and Big-data Services (SICBS 2018), Guilin, China, December 14-16, 2018.
- *Tutorial on Visual Cryptography*, 8th IEEE International Workshop on Information Forensics and Security (WIFS) 2016, Abu Dhabi, UAE, December 4-7, 2016.

- *Panel on Big data security: issues and challenges.*, SIN '16 9th International Conference on Security of Information and Networks. Newark, NJ, USA, July 20 - 22, 2016.
- *Visual Cryptography: Watermarking and Novel Applications*  
invited by Prof. Feng Liu, Director of the Executive Office of State Key Laboratory of Information Security, Institute of Information Engineering Chinese Academy of Sciences, Beijing China, 17 October 2013
- *Visual Cryptography: Research Issues and Novel Applications*  
invited by Prof. T. Fournel, Université de Saint-Etienne, Laboratoire Hubert Curien Saint-Etienne, France, 26 September 2012
- *Data Analysis with Privacy Constraints*  
invited speaker at CRiSIS 2011, 6th International Conference on. Risks and Security of Internet and Systems, Timisoara, Romania, 26-28 September 2011
- *RFID Security in Business Applications*  
Workshop on RFID Security, Akademia Ekonomiczna, Wroclaw, Poland, March 2008
- *Cryptographic Protocols for Internet Services*  
3rd International School on Foundations of Security Analysis and Design (FOSAD 2002), Bertinoro (FC), Italia, September 2002.
- *A Methodology for the Specification of Java Components and Architectures*  
System Integration, Dagstuhl Seminar 99111, Dagstuhl, Germany, March 1999.
- *Formal Specification of Component-Based Java Applications.*  
INRIA-IRISA, University of Rennes, Francia, invited by prof. V. Issarny, October 1998.

#### 5.4.2 Partecipazione in qualità di relatore a Convegni Scientifici

- ICISSP 2024 – 10th International Conference on Information Systems Security and Privacy, Rome, Italy, February 26-28, 2024
- DBDM 2020 - 5th IEEE International Workshop on Distributed Big Data Management in conjunction with COMPSAC 2020, Madrid, Spain, July 13-17, 2020 (virtual)
- STM 2019 – Security and Trust Management - 15th International Workshop, Luxembourg City, Luxembourg, September 26-27, 2019,
- SICBS 2018 – 2nd International Conference on Security with Intelligent Computing and Big-data Services, Guilin, China, December 14-16, 2018.
- ESAS 2018 – e-Health Systems and Web Technologies, 13h International Workshop, Tokyo, Japan - July 23-27, 2018
- ICISSP 2018 – 4th International Conference on Information Systems Security and Privacy, Madeira, Portugal, January 22-24, 2018
- ICISSP 2016 – 2nd International Conference on Information Systems Security and Privacy, Rome, Italy, 19-21 February, 2016
- IIH-MSP 2013 – 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, China, October 2013.
- SETOP 2012 – 5th International Workshop on Autonomous and Spontaneous Security (in conjunction with ESORICS 2012), Pisa, Italy, September 2012
- STM 2012 – 8th International Workshop on Security and Trust Management (in conjunction with ESORICS 2012), Pisa, Italy, September 2012

- ACM SAC 2010 – 25th Symposium On Applied Computing Saint Moritz, Switzerland, March 2010.
- SAPSE 2010 – 2nd IEEE International Workshop on Security Aspects of Process and Services Engineering (in conjunction with COMPSAC 2010) Seoul, Korea, July 2010.
- STPSA 2008 – 3rd IEEE International Workshop on Security, Trust, and Privacy for Software Application (in conjunction with COMPSAC 2008), Turku, Finland, July 2008.
- NTMS 2007 – International Conference on New Technologies, Mobility and Security, Paris, France, May 2007.
- ISCC 2006 – IEEE Symposium on Computers and Communications Pula, Italy, June 2006.
- CANS 2005 – International Conference on Cryptology and Network Security , Xiamen, China, December 2005.
- SAINT 2005 – International Symposium on Applications and the Internet, Trento, Italy, January 2005.
- SCN 2004 – Fourth International Conference on Security in Communication Networks, Amalfi, Italy, September 2004.
- CSES 2004 – International Workshop on Certification and Security in Inter-Organizational E-Services, Toulouse, France, August 2004.
- ITCC'04 – IEEE International Conference on Information Technology, Las Vegas, USA, April 2004.
- ITCTS'03 – Italian Conference on Theoretical Computer Science, Bertinoro, Italy, September 2003.
- ISCC'03 – IEEE Symposium on Computers and Communications, Antalya, Turkey, July 2003.
- ITW'03 – IEEE Information Theory Workshop , La Sorbonne, Paris, France, March-April 2003.
- SEKE'02 – 14th International Conference on Software Engineering and Knowledge Engineering, Ischia, Italy, July 2002.
- WWW'02 – 11th World Wide Web Conference , Honolulu, Usa, May 2002.
- ICISC 2001 – 4th International Conference on Information Security and Cryptology, Seoul, Korea, December 2001.
- ICTCS'01 – 7th Italian Conference on Theoretical Computer Science, Torino, Italy, October 2001.
- ECOOP'99 – Workshop on Formal Techniques for Java Programs, Lisbon, Portugal, June 1999.
- Dagstuhl 99 – Seminar on System Integration, Dagstuhl, Germany, March 1999
- FMOODS'99 – Third International Conference on Formal Methods for Open Object-Based Distributed Systems Florence, Italy, February 15-18, 1999
- RENOIR 98 – Research Training "Mini-Workshop" Bommerholz, Germany, January 1998
- ESEC/FSE 97 – Sixth European Software Engineering Conference and Fifth ACM SIG-SOFT Symposium on the Foundations of Software Engineering, Zurich, Switzerland, 22-25 September 1997
- Grenoble 97 – Methods and Tools for the Verification of Infinite State Systems Grenoble, France, 23-25 Marzo 1997.

- APPIA-GULP-PRODE'96 – Joint Conference on Declarative Programming, San Sebastian, Spain, 15-18 July 1996.

## 5.5 Pubblicazioni

### Editore di Libri e Special Issues

- [1] Shi Dong, Stelvio Cimato, Joarder Kamruzzaman, and Yongsheng Hao Special issue "Real-Time Image Steganography and Steganalysis" Journal of Electronic Imaging, Vol. 33, Issue 1, 011001 (February 2024). <https://doi.org/10.1117/1.JEI.33.1.011001>
- [2] J.C.N. Yang, S. Cimato, Lizhi Xiong Special issue "Information Theory and Its Applications in Multimedia Security and Processing", in Entropy - MDPI, 2022 ISSN 1099-4300
- [3] Yimin Yang, James C.N. Yang, Cheonshik Kim, Stelvio Cimato, Gaurav Bhatnagar, Special issue "Computational Intelligence Techniques for Information Security and Forensics in IoT Environments" in Wireless Communications and Mobile Computing, Wiley - Hindawi ISSN:1530-8669E-ISSN:1530-8677 (indicizzato Scopus)
- [4] Zhili Zhou, Ching-Nung Yang, Cheonshik Kim, Stelvio Cimato: Special issue "Deep learning for real-time information hiding and forensics" Journal of Real-Time Image Processing, Volume 17, Number 1, February 2020, Springer, ISSN: 1861-8200 (indicizzato Scopus)
- [5] James Ching-Nung Yang, Cheonshik Kim, Stelvio Cimato: Special issue "Computing Methods in Steganography and Multimedia Security" Mathematics, vol. 8, MDPI, ISSN: 2227-7390
- [6] S. Cimato and C.N. Yang *Visual Cryptography and Secret Image Sharing*, CRC Press, USA, 2011. ISBN: 9781439837214

### Editore di Atti di Convegni

- [7] Vladimir Getov, Jean-Luc Gaudiot, Nariyoshi Yamai, Stelvio Cimato, J. Morris Chang, Yuichi Teranishi, Ji-Jiang Yang, Hong Va Leong, Hossain Shahriar, Michiharu Takemoto, Dave Towey, Hiroki Takakura, Atilla Elçi, Susumu Takeuchi, Satish Puri: 43rd IEEE Annual Computer Software and Applications Conference, COMPSAC 2019, Milwaukee, WI, USA, July 15-19, 2019, Volume 1-2. IEEE 2019, ISBN 978-1-7281-2607-4
- [8] S. Reisman, S. I. Ahamed, C. Demartini, T. M. Conte, L. Liu, W. R. Claycomb, M. Nakamura, E. Tovar, S. Cimato, C. Lung, H. Takakura, J. Yang, T. Akiyama, Z. Zhang, K. Hasan, 2018 IEEE 42nd Annual Computer Software and Applications Conference, COMPSAC 2018, Tokyo, Japan, 23-27 July 2018, Volume 1, IEEE Computer Society, 2018, ISBN 978-1-5386-2667-2
- [9] S. Reisman, S. I. Ahamed, C. Demartini, T. M. Conte, L. Liu, W. R. Claycomb, M. Nakamura, E. Tovar, S. Cimato, C. Lung, H. Takakura, J. Yang, T. Akiyama, Z. Zhang, K. Hasan, 41st IEEE Annual Computer Software and Applications Conference, COMPSAC 2017, Turin, Italy, July 4-8, 2017. Volume 1, IEEE Computer Society, 2017, ISBN 978-1-5386-0367-3
- [10] S. Reisman, S. I. Ahamed, C. Demartini, T. M. Conte, L. Liu, W. R. Claycomb, M. Nakamura, E. Tovar, S. Cimato, C. Lung, H. Takakura, J. Yang, T. Akiyama, Z. Zhang, K. Hasan, 41st IEEE Annual Computer Software and Applications Conference, COMPSAC 2017, Turin, Italy, July 4-8, 2017. Volume 2, IEEE Computer Society, 2017.



- [11] S. Jajodia, P. Samarati and S. Cimato, editors *Proceedings of the 23rd International Information Security Conference (SEC 2008)*, IFIP Series, Springer Verlag, New York, USA, 2008. ISBN: 9780387096988
- [12] C. Blundo and S. Cimato, editors *Security in Communication Networks, Fourth International Conference, (SCN 2004)*, Vol. 3352 di Lecture Notes in Computer Science, Springer Verlag, New York, USA, 2005. ISBN 3-540-24301-1
- [13] S. Cimato, C. Galdi and P. Persiano, editors *Security in Communication Networks, Third International Conference, (SCN 2002)*, Vol. 2576 di Lecture Notes in Computer Science, Springer Verlag, New York, USA, 2003. ISBN: 3-540-00420-3

## Riviste Internazionali

- [14] C. Blundo, S. Cimato, "Role mining under User-Distribution cardinality constraint", *Journal of Information Security and Applications*, vol. 78, 2023, pp. 103611. ISSN: 2214-2126, <https://doi.org/10.1016/j.jisa.2023.103611>
- [15] C. Blundo, S. Cimato and L. Siniscalchi, "Heuristics for constrained role mining in the post-processing framework", *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 8, 2023, pp. 9925–9937. ISSN: 1868-5137, <http://dx.doi.org/10.1007/s12652-021-03648-1>
- [16] C. Blundo, S. Cimato and L. Siniscalchi, "Role Mining Heuristics for Permission-Role-Usage Cardinality Constraints", *Comput. J.*, vol. 65, no. 6, 2022, pp. 1386–1411. ISSN: 0010-4620, <http://dx.doi.org/10.1093/comjnl/bxaa186>
- [17] A. Bernasconi, S. Cimato, V. Ciriani, M. Molteni, "Multiplicative Complexity of XOR Based Regular Functions", *IEEE Transactions on Computers*, 2022. ISSN: 0018-9340, <http://dx.doi.org/10.1109/TC.2022.3141249>
- [18] S. Cimato, G. Gianini, M. Sepehri, R. Asal, E. Damiani, "A cryptographic cloud-based approach for the mitigation of the airline cargo cancellation problem", *Journal of Information Security and Applications*, vol. 51, 2020, pp. 1-21. ISSN: 2214-2126, <https://doi.org/10.1016/j.jisa.2020.102462>
- [19] C. Blundo, S. Cimato and L. Siniscalchi, "Managing Constraints in Role Based Access Control", *IEEE Access*, vol. 8, 2020, pp. 140497- 140511. ISSN: 2169-3536, <http://dx.doi.org/10.1109/ACCESS.2020.3011310>
- [20] E. Damiani, V. Bellandi, S. Cimato, G. Gianini and A. Zilli, "Towards Economics-Aware Risk Assessment on the cloud", *IEEE Security and Privacy*, vol. 13, no. 6, pp. 30-37, IEEE Computer Society, New York, USA, 2015. ISSN 1540-7993 <http://dx.doi.org/10.1109/MSP.2015.138>
- [21] M. Sepehri, S. Cimato and E. Damiani, "Privacy-Preserving Query Processing by Multi-Party Computation", *The Computer Journal*, vol. 58(10), pp. 2195-2212, Oxford University Press, Oxford, UK, 2015. ISSN: 0010-4620 doi:10.1093/comjnl/bxu093
- [22] M. Hadavi, R. Jalili, E. Damiani, and S. Cimato, "Security and searchability in secret sharing-based data outsourcing", *International Journal of Information Security*, vol. 14 (6), pp. 513-529, 2015. ISSN:1615-5262 doi:10.1007/s10207-015-0277-x

- [23] E. Damiani, S. Cimoto and G. Gianini, “A risk model for cloud processes”, *The ISecure International Journal on Information Security*, vol.6(2), pp. 99-123, ISC, 2014. ISSN: 2008-2045
- [24] S. Cimoto, James C.N. Yang, and Chih-Cheng Wu, “Visual Cryptography Based Watermarking” in *Transactions on Data Hiding and Multimedia Security*, vol 8363, pp. 91-109, Springer, USA, 2014. ISBN: 978-3-642-55045-4 <https://doi.org/10.1007/978-3-642-55046-1>
- [25] S. Abbasi, S. Cimoto and E. Damiani, “Clustering Models in Secure Clustered Multiparty Computation” in *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol 4:2, pp. 63-76, ISYOU, June 2013. ISSN: 2093-5374 10.22667/JOWUA.2013.06.31.063
- [26] F. Kerschbaum, A. Schropfer, A. Zilli, R. Pibernik, O. Catrina, S. de Hoogh, B. Schoenmakers, S. Cimoto and E. Damiani, “Secure Collaborative Supply-Chain Management” in *IEEE Computer*, vol 9, pp. 38-43, IEEE, September 2011. ISSN: 0018-9162 doi:10.1109/MC.2011.224
- [27] C. Blundo, S. Cimoto, S. De Capitani di Vimercati, A. De Santis, S. Foresti, S. Paraboschi, and P. Samarati, “Managing Key Hierarchies for Access Control Enforcement: Heuristic Approaches” in *Computers & Security*, vol 29(5), pp 533-547, Elsevier, Essex, UK, July 2010. ISSN: 0167-4048 doi:10.1016/j.cose.2009.12.006
- [28] S. Cimoto, R. Sassi and F. Scotti, “Biometrics and Privacy” in *Recent Patents on Computer Science* Volume 1 (2):98-109, Bentham Publisher, USA, 2008. ISSN: 1874-4796
- [29] S. Cimoto, R. De Prisco and A. De Santis, “Colored visual cryptography without color darkening” in *Theoretical Computer Science* 374 (1-3): 261-276, Elsevier, Essex, UK, 2007. ISSN: 0304-3975 doi:10.1016/j.tcs.2007.01.006
- [30] C. Blundo, S. Cimoto and A. De Santis, “Visual Cryptography Schemes with Optimal Pixel Expansion” in *Theoretical Computer Science*, 369: 169-182, Elsevier, Essex, UK, 2006. ISSN: 0304-3975 doi:10.1016/j.tcs.2006.08.008
- [31] S. Cimoto, R. De Prisco and A. De Santis, “Probabilistic Visual Cryptography Schemes” in *The Computer Journal*, 49: 97-107, Oxford University Press, Oxford, UK, 2006. ISSN: 0010-4620 doi:10.1093/comjnl/bxh152
- [32] S. Cimoto, A. Cresti and P. D’Arco, “A Unified Model for Unconditionally Secure Key Distribution” in *Journal of Computer Security*, 14(1), pp. 45-64, IOS Press, Amsterdam, The Netherlands, 2006. ISSN: 0926-227X, doi:10.3233/JCS-2006-14102
- [33] S. Cimoto, A. De Santis and U. Ferraro, “Overcoming the Obfuscation of Java Programs by Identifiers Renaming”, in *Journal of Systems and Software*, Vol. 78, Issue 1, pp 60-72, Elsevier, New York, USA, 2005. ISSN: 0164-1212, doi:10.1016/j.jss.2004.11.019
- [34] S. Cimoto, R. De Prisco and A. De Santis, “Optimal Colored Threshold Visual Cryptography Schemes” in *Designs, Codes and Cryptography*, Vol 35, N. 3, pp. 311-335, Kluwer Academic Publishers, Norwell, USA, 2005. ISSN: 0925-1022 doi:10.1007/s10623-003-6741-z
- [35] S. Cimoto, A. De Santis, A. L. Ferrara, and B. Masucci, “Ideal Contrast Visual Cryptography Schemes with Reversing”, in *Information Processing Letters*, Volume: 93, Issue: 4 ,pp. 199-206, Elsevier, Amsterdam, The Netherlands, 2005. ISSN: 0020-0190 10.1016/J.IPL.2004.10.011

- [36] C. Blundo, S. Cimato and A. De Bonis, “Secure E-Coupons”, in *Electronic Commerce Research*, vol 5, No. 1, pp. 117-139 Kluwer Academic Publishers, Norwell MA, USA, 2005. ISSN: 1389-5753 doi:10.1023/B:ELEC.0000045976.24984.48
- [37] C. Blundo and S. Cimato, “A Software Infrastructure for Authenticated Web Metering”, in *IEEE Computer*, Vol. 37, No. 4, pp. 28-33, IEEE Computer Society Press, Los Alamitos CA, USA, 2004. ISSN: 0018-9162, doi:10.1109/MC.2004.1297298
- [38] C. Blundo, S. Cimato, R. De Prisco and A. Ferrara, “Modeling A Certified Email Protocol using I/O Automata”, *Electronic Notes in Theoretical Computer Science*, vol. 99, pp. 339-359, Elsevier, 2004. ISSN: 1571-0661 doi:10.1016/j.entcs.2004.02.015
- [39] C. Blundo, S. Cimato and B. Masucci, “A Note on Optimal Metering Schemes”, *Information Processing Letters*, vol. 84/6, pp. 319–326, Elsevier, Amsterdam, The Netherlands, 2002. ISSN: 0020-0190, doi:10.1016/S0020-0190(02)00321-6
- [40] P. Ciancarini, S. Cimato and C. Mascolo, “Engineering Formal Requirements: an Analysis and Testing Method for Z Documents”, *Annals of Software Engineering*, vol. 3, pp. 189–220, Kluwer Academic Publisher, The Netherlands, 1997. ISSN: 1022-7091 10.1023/A:1018965316985

### Capitoli in libri

- [41] L. Mauri, S. Cimato and E. Damiani, ”Untangling the XRP Ledger: Insights and Analysis”, in *Information Systems Security and Privacy*, S. Furnell, P. Mori, E. Weippl, O. Camp, Eds., Cham: Springer International Publishing, 2022, pp. 48–72, ISBN: 978-3-030-94899-3, ISSN: 1865-0929, doi:10.1007/978-3-030-94900-6\_3
- [42] S. Cimato, E. Damiani, ”Some Ideas on Privacy-Aware Data Analytics in the Internet-of-Everything”, in *From Database to Cyber Security - Essays Dedicated to Sushil Jajodia on the Occasion of His 70th Birthday*, P. Samarati, I. Ray, I. Ray, Eds., Springer, 2018, pp. 113–124, ISBN: 9783030048334, ISSN: 0302-9743, doi:10.1007/978-3-030-04834-1\_6
- [43] S. Cimato, V. Ciriani, M. Moroni “Minimization of ESOP forms for secure computation”. In: (a cura di): B. Steinbach, *Problems and new solutions in the Boolean domain*. p. 241-254, Cambridge Scholars Publishing, ISBN: 1443889474
- [44] E. Damiani, V. Bellandi, S. Cimato, G. Gianini, “Possibilistic assessment of process-related disclosure risks on the cloud”, in *Computational Intelligence and Quantitative Software*, W. Pedrycz, G. Succi, A. Sillitti, Eds., Springer, in press, pp. 385-405, 2015. , ISBN: 9783319259628, ISSN: 1860-949X, doi:10.1007/978-3-319-25964-2\_9
- [45] S. Cimato, S. Mella and R. Susella, “Partial Key Exposure Attacks on RSA with Exponent Blinding”, in *E-Business and Telecommunications - 12th International Joint Conference, ICETE 2015*, Colmar, France, July 20-22, 2015, Revised Selected Papers, 2015, pp. 364–385.
- [46] S. Cimato, J. C. N. Yang, C. C. Wu (2014). Visual cryptography based watermarking. In: (a cura di): Y.Q. Shi;F. Liu;W. Yan, *Transactions on data hiding and multimedia security IX*. vol. 8363, p. 91-109, Berlin:SPRINGER, ISBN: 9783642550454, doi:10.1007/978-3-642-55046-1\_6
- [47] S. Cimato “Image Watermarking Using Visual Cryptography”, in *Steganography and Watermarking*, Nova Science Publishers, USA, September 2012. ISBN: 9781626183131

- [48] S. Cimoto, R. De Prisco, and A. de Santis “Visual Cryptography for Color Images”, in *Visual Cryptography and Secret Image Sharing*, CRC Press, Boca Raton, USA, August 2011. ISBN: 9781439837214
- [49] S. Cimoto, R. De Prisco, and A. de Santis “Probabilistic Visual Cryptography”, in *Visual Cryptography and Secret Image Sharing*, CRC Press, Boca Raton, USA, August 2011. ISBN: 9781439837214
- [50] S. Cimoto, M. Gamassi, V. Piuri, R. Sassi, F. Scotti, “Privacy in Biometrics” in *Biometrics: Theory, Methods and Applications*, N. Boulgoris, E. Micheli-Tzanakou, K. Patanionis editors (IEEE/Wiley press), 2009 ISBN: 9780470247822 doi:10.1002/9780470522356.ch25
- [51] C. Blundo, S. Cimoto and B. Masucci, “Secure Metering Schemes”, in *Network Security*, Scott C.-H. Huang, David MacCallum, Ding-Zhu Du (editors), Springer-Verlag New York Inc., 2008. ISBN: 978-0-387-73820-8 doi:10.1007/978-0-387-73821-5\_1

### Conferenze Internazionali

- [52] J. Shahid, S. Cimoto, M. Zia, “A Sharded Blockchain Architecture for Healthcare Data”. In: (a cura di): H. Shahriar;H. Ohsaki;M. Sharmin;D. Towey;AKM J. A. Majumder Yoshiaki Hori;J.-J. Yang;M. Takemoto;N. Sakib;R. Banno;S. Iqbal Ahamed, COMPSAC. vol. 1, p. 1794-1799, Institute of Electrical and Electronics Engineers (IEEE), ISBN: 979-8-3503-7696-8, Osaka (Japan), 2024, doi:10.1109/compsac61105.2024.00283
- [53] A. Migliore, S. Cimoto, G. Trucco, ”Efficient Secure Computation of Edit Distance on Genomic Data”. In: (a cura di): G. Lenzini;P. Mori;S. Furnell, Proceedings of the ICIS-SP. ICISSP, p. 878-883, SciTePress, ISBN: 9789897586835, ISSN: 2184-4356, Roma, 2024, doi:10.5220/0012459400003648
- [54] E. Bellini, I. Aversa, S. Cimoto, A. Esposito, ”A Blockchain-based Trustworthy Cloud Services Digital Ecosystem”, in IEEE International Conference on Cyber Security and Resilience, CSR 2022, Rhodes, Greece, July 27-29, 2022, IEEE, pp. 118–124. ISBN: 978-1-6654-9952-1, Rhodes, 2022, doi:10.1109/CSR54599.2022.9850336
- [55] L. Brunie, S. Ben Mokhtar, D. Brac de la Perrière, D. Fabrègue, L.Tondu, A. Cordier, V. Delplanque, A. Bertrand, O. Coueffe, H. Kosch, E. Damiani, S. Cimoto, I.A. Awada, A. Olaru, R. Wossidlo,G. Fiorentino, L. Lombardo, F.S. Nucci, O. Cramariuc, Oana. Fostering student entrepreneurship mindset through the embedding of international student teams into start-ups and the study of company-driven open questions. In: EDULEARN22 Proceedings. EDULEARN PROCEEDINGS, p. 4544-4549, IATED, ISBN: 978-84-09-42484-9, ISSN: 2340-1117, Palma, 2022, doi:10.21125/edulearn.2022.1087
- [56] L. Brunie, S. Ben Mokhtar, D. Brac de la Perrière, D. Fabrègue, L.Tondu, A. Cordier, V. Delplanque, A. Bertrand, O. Coueffe, H. Kosch, E. Damiani, S. Cimoto, I.A. Awada, A. Olaru, R. Wossidlo,G. Fiorentino, L. Lombardo, F.S. Nucci, O. Cramariuc, Oana. Training future it leaders in a collaborative and multicultural setting. In: EDULEARN22 Proceedings. EDULEARN PROCEEDINGS, vol. 1, p. 5318-5321, IATED, ISBN: 978-84-09-42484-9, ISSN: 2340-1117, Palma, 2022, doi:10.21125/edulearn.2022.1258
- [57] Brunie, Lionel, Cimoto, Stelvio, Cramariuc, Oana (2021). Key competences expected of future it leaders in a multicultural and digital Europe. In: EDULEARN21 Proceedings. EDULEARN

PROCEEDINGS, vol. 1, p. 7635-7641, IATED, ISBN: 978-84-09-31267-2, ISSN: 2340-1117, Online, 2021, doi:10.21125/edulearn.2021.1552

- [58] E. Bellini, S. Cimato, E. Damiani, B. D. Martino, A. Esposito, "Towards a Trustworthy Semantic-Aware Marketplace for Interoperable Cloud Services", in Complex, Intelligent and Software Intensive Systems - Proceedings of the 15th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2021), Asan, Korea, 1-3 July 2021, L. Barolli, K. Yim, T. Enokido, Eds., Springer, pp. 606-615. ISBN: 9783030797249, ISSN: 2367-3370, 2021, doi:10.1007/978-3-030-79725-6\_61
- [59] L. Mauri, E. Damiani and S. Cimato, "Be Your Neighbor's Miner: Building Trust in Ledger Content via Reciprocally Useful Work", in Proceedings of IEEE International Conference on Cloud Computing 2020, IEEE CLOUD 2020, Octobr 18-24, 2020, p. 53-62, IEEE, ISBN: 9781728187808, ISSN: 2159-6190, Beijing, 2020, doi:10.1109/CLOUD49709.2020.00021
- [60] C. Braghin, S. Cimato, E. Damiani, F. Frati, E. Riccobene, S. Astaneh, "Towards the Monitoring and Evaluation of Trainees' Activities in Cyber Ranges", in Model-driven Simulation and Training Environments for Cybersecurity - Second International Workshop, MSTEC 2020, In: (a cura di): G. Hatzivasilis;S. Ioannidis, Model-driven Simulation and Training Environments for Cybersecurity. LECTURE NOTES IN ARTIFICIAL INTELLIGENCE, vol. 12512, p. 79-91, Springer, ISBN: 9783030624323, ISSN: 0302-9743, Guildford, 2020, doi:10.1007/978-3-030-62433-0\_5
- [61] L. Mauri, S. Cimato and E. Damiani, "A Formal Approach for the Analysis of the XRP Ledger Consensus Protocol", in Proceedings of the 6th International Conference on Information Systems Security and Privacy, ICISSP 2020, Valletta, Malta, February 25-27, 2020, S. Furnell, P. Mori, E. R. Weippl, O. Camp, Eds., SCITEPRESS, pp. 52-63. ISBN: 9789897583995, La Valletta, 2020, doi:10.5220/0008954200520063
- [62] A. Bernasconi, S. Cimato, V. Ciriani, M. C. Molteni, "Multiplicative Complexity of Autosymmetric Functions: Theory and Applications to Security", in 57th ACM/IEEE Design Automation Conference, DAC 2020, San Francisco, CA, USA, July 20-24, 2020, IEEE, pp. 1-6. ISBN: 9781728110851, San Francisco, 2020, doi:10.1109/DAC18072.2020.9218492
- [63] S. Cimato, S. Nicoló, "Towards Efficient and Secure Analysis of Large Datasets", in 44th IEEE Annual Computers, Software, and Applications Conference, COMPSAC 2020, Madrid, Spain, July 13-17, 2020, IEEE, pp. 1351-1356. ISBN: 9781728173030, Madrid, 2020, doi:10.1109/COMPSAC48688.2020.00-68
- [64] S. Cimato, V. Ciriani, E. Damiani, M. Ehsanpour, "An OBDD-Based Technique for the Efficient Synthesis of Garbled Circuits", in Security and Trust Management - 15th International Workshop, STM 2019, Luxembourg City, Luxembourg, September 26-27, 2019, Proceedings, pp. 158-167. LECTURE NOTES IN COMPUTER SCIENCE, vol. 11738, p. 158-167, Springer, ISBN: 9783030315108, ISSN: 0302-9743, Luxembourg, 2019, doi:10.1007/978-3-030-31511-5\_10
- [65] C. Braghin, S. Cimato, E. Damiani, F. Frati, L. Mauri, E. Riccobene, "A Model Driven Approach for Cyber Security Scenarios Deployment", in Computer Security - ESORICS 2019 International Workshops, Iosec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers, A. P. Fournaris, M. Athanatos, K. Lampropoulos, S. Ioannidis, G. Hatzivasilis, E. Damiani, H. Abie, S. Ranise, L. Verde-

- rame, A. Siena, J. García-Alfaro, Eds., . LECTURE NOTES IN ARTIFICIAL INTELLIGENCE, vol. 11981, p. 107-122, Springer, ISBN: 9783030420505, Luxembourg City, 2019, doi:10.1007/978-3-030-42051-2\_8
- [66] C. Braghin, S. Cimato, S. R. Cominesi, E. Damiani, L. Mauri, "Towards Blockchain-Based E-Voting Systems", in Business Information Systems Workshops - BIS 2019 International Workshops, Seville, Spain, June 26-28, 2019, Revised Papers, pp. 274-286. LECTURE NOTES IN BUSINESS INFORMATION PROCESSING, vol. 373, p. 274-286, Springer, ISBN: 9783030366902, ISSN: 1865-1348, Siviglia, 2019, doi:10.1007/978-3-030-36691-9\_24
- bibitemwallet1 P.J Hounbo, J, Hounsou, E. Damiani, R. Asal, S. Cimato, F. Frati, C.Y. Yeun, "Embedding a Digital Wallet to Pay-with-a-Selfie, Defining the System Architecture as Blockchain Based". In: (a cura di): R. Zitouni;M. Agueh, Emerging Technologies for Developing Countries. LECTURE NOTES OF THE INSTITUTE FOR COMPUTER SCIENCES, SOCIAL INFORMATICS AND TELECOMMUNICATIONS ENGINEERING, vol. 260, p. 109-124, Springer, ISBN: 9783030051976, ISSN: 1867-8211, Cotonou, 2018, doi:10.1007/978-3-030-05198-3\_10
- [67] P.J Hounbo, J, Hounsou, E. Damiani, R. Asal, S. Cimato, F. Frati, C.Y. Yeun, Embedding a Digital Wallet to Pay-with-a-Selfie, from Functional Requirements to Prototype. In: (a cura di): R. Zitouni;M. Agueh, Emerging Technologies for Developing Countries. LECTURE NOTES OF THE INSTITUTE FOR COMPUTER SCIENCES, SOCIAL INFORMATICS AND TELECOMMUNICATIONS ENGINEERING, vol. 260, p. 47-56, Springer, ISBN: 9783030051976, ISSN: 1867-8211, Cotonou, 2018, doi:10.1007/978-3-030-05198-3\_4
- [68] C. Braghin, S. Cimato, E. Damiani, M. Baronchelli, "Designing Smart-Contract Based Auctions", in Security with Intelligent Computing and Big-data Services, Proceedings of SICBS 2018 - International Conference on Security with Intelligent Computing and Big-data Services, C. Yang, S. Peng, L. C. Jain, Eds., Springer International Publishing, 2019, ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING, vol. 895, p. 54-64, Springer, ISBN: 9783030169459, ISSN: 2194-5357, Guilin, 2018, doi:10.1007/978-3-030-16946-6\_5
- [69] C. Braghin, S. Cimato, A. Della Libera (2018). Are mHealth Apps Secure? : A Case Study. In: IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC 2018). p. 335-340, IEEE, ISBN: 9781538626665, Tokyo, 2018, doi:10.1109/COMPSAC.2018.10253
- [70] L. Mauri, S. Cimato and E. Damiani, "A Comparative Analysis of Current Cryptocurrencies", in Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, Madeira, Portugal, January 22-24, 2018, pp. 127-138. ISBN: 9789897582820, Madeira, 2018, doi:10.5220/0006648801270138
- [71] C. Blundo, S. Cimato, L. Siniscalchi, Luisa, "PostProcessing in Constrained Role Mining". In: (a cura di): H. Yin;D. Camacho;P. Novais;A.J. Tallón-Ballesteros, Intelligent Data Engineering and Automated Learning – IDEAL 2018. LECTURE NOTES IN COMPUTER SCIENCE, vol. 11314, p. 204-214, Springer, ISBN: 9783030034924, ISSN: 0302-9743, Madrid, 2018, doi:10.1007/978-3-030-03493-1\_22
- [72] S. Cimato, V. Ciriani, E. Damiani, M. Ehsanpour, "A Multiple Valued Logic Approach for the Synthesis of Garbled Circuits", in 2018 IFIP/IEEE 25th International Conference on Very Large Scale Integration, VLSI-SoC 2017, ABU Dhabi, UAE, October 22-25, 2018, pp. 232-236. IEEE, ISBN: 9781538628805, doi:10.1109/VLSI-SoC.2017.8203495

- [73] M. Ehsanpour, S. Cimoto, V. Ciriani, E. Damiani, “Exploiting Quantum Gates in Secure Computation”, in *Euromicro Conference on Digital System Design, DSD 2017*, Vienna, Austria, August 30 - Sept. 1, 2017, pp. 291–294. IEEE, ISBN: 9781538621462, doi:10.1109/DSD.2017.53
- [74] C. Blundo, S. Cimoto and L. Siniscalchi, “PRUCC-RM: Permission-Role-Usage Cardinality Constrained Role Mining”, in *41st IEEE Annual Computer Software and Applications Conference, COMPSAC 2017*, Turin, Italy, July 4-8, 2017. Volume 2, pp. 149–154. ISBN: 9781538603673, doi:10.1109/COMPSAC.2017.195
- [75] M. Sepehri, S. Cimoto and E. Damiani, “Efficient Implementation of a Proxy-based Protocol for Data Sharing on the Cloud”, in *Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing, SCC at AsiaCCS 2017*, Abu Dhabi, United Arab Emirates, April 2, 2017, pp. 67–74. ACM, ISBN: 9781450349703, doi:10.1145/3055259.3055271
- [76] E. Damiani, P. J. Hounsgbo, J. Hounsou, R. Asal, S. Cimoto, F. Frati, D. Shehada, C. Y. Yeun, “Porting the Pay with a (Group) Selfie (PGS) payment system to crypto currency”. In: (a cura di): F. Belqasmi;H. Harroud;M. Agueh;R. Dssouli;F. Kamoun, *Emerging Technologies for Developing Countries. LECTURE NOTES OF THE INSTITUTE FOR COMPUTER SCIENCES, SOCIAL INFORMATICS AND TELECOMMUNICATIONS ENGINEERING*, vol. 206, p. 159-168, Springer Verlag, ISBN: 9783319678368, ISSN: 1867-8211, Marrakech, 2017, doi:10.1007/978-3-319-67837-5\_15
- [77] C. Yang, S. Cimoto, J. Wu, S. Cai, “3-Out-of-n Cheating Prevention Visual Cryptographic Schemes”, in *Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP 2016*, Rome, Italy, February 19-21, 2016., pp. 400–406. ISBN: 9789897581670, Roma, 2016, doi:10.5220/0005740504000406
- [78] S. Cimoto, E. Damiani, S. Mella, C. Yang, “Key Recovery in Public Clouds: A Survey on Cross-VM Side Channel Attacks”, in *Cloud Computing and Security - Second International Conference, ICCCS 2016*, Nanjing, China, July 2016 *LECTURE NOTES IN COMPUTER SCIENCE*, vol. 10039, p. 456-467, Springer, ISBN: 9783319486703, ISSN: 0302-9743, doi:10.1007/978-3-319-48671-0\_40
- [79] M. Sepehri, S. Cimoto, E. Damiani, C. Y. Yeuny, “Data Sharing on the Cloud: A Scalable Proxy-Based Protocol for Privacy-Preserving Queries”, in *Proceedings of the 7th IEEE International Symposium on Ubisafe Computing in conjunction with 14th IEEE Conference on Trust, Security and Privacy in Computing and Communications, TrustCom/BigDataSE/ISPA*, Helsinki, Finland, August 20-22, 2015, Volume 1, pp. 1357–1362. ISBN: 9781467379526, Helsinki, 2015, doi:10.1109/Trustcom.2015.530
- [80] S. Cimoto, E. Damiani, F. Frati, J. T. Hounsou, J. Tandjiékpon, “Paying with a Selfie: a Hybrid Micro-Payment Framework Based on Visual Cryptography”, in *7th EAI International Conference on e-Infrastructure and e-Services for Developing Countries (Afri-comm15)*, Cotonou, Benin, December 15–16, 2015. *LECTURE NOTES OF THE INSTITUTE FOR COMPUTER SCIENCES, SOCIAL INFORMATICS AND TELECOMMUNICATIONS ENGINEERING*, vol. 171, p. 136-141, Springer, ISBN: 9783319436968, ISSN: 1867-8211, doi:10.1007/978-3-319-43696-8\_15
- [81] S. Cimoto, S. Mella, R. Susella, “Partial Key Exposure Attacks on RSA with Exponent Blinding.”, in *E-Business and Telecommunications - 12th International Joint Conference (ICE-*

- TE), pp. 364-385, COMMUNICATIONS IN COMPUTER AND INFORMATION SCIENCE, vol. 585, p. 364-385, Springer, ISBN: 9783319302218, ISSN: 1865-0929, Colmar, 2015, doi:10.1007/978-3-319-30222-5\_17
- [82] S. Cimato, S. Mella and R. Susella, “New Results for Partial Key Exposure on RSA with Exponent Blinding”, in *SECURITY 2015 - Proceedings of the 12th International Conference on Security and Cryptography*, Colmar, Alsace, France, pp. 136–147, 20-22 July, 2015. ISBN: 9789897581175, doi:10.5220/0005571701360147
  - [83] S. Cimato, V. Ciriani, and M. Moroni, “ESOP Synthesis for Secure Computation”, in *10th International Workshop on Boolean Problems (IWSBP14)*, Freiberg, Germany, 17-19 September 2014. ISBN: 978-3-86012-488-8, 2014
  - [84] S. Cimato, “Visual Cryptography Schemes for Graph Based Access Structures”, in *Proceedings of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2013)* page 365-368, Beijing, China, 15-18 October 2013. ISBN: 9780769551203 doi:10.1109/IIH-MSP.2013.98
  - [85] M. Sepehri, S. Cimato, E. Damiani, “A Multi-Party Protocol for Privacy-Preserving Range Queries”, in *Proceedings of the 10th Secure Data Management Workshop (SDM 2013)*, Riva del Garda (Trento), Italy, August 2013. LECTURE NOTES IN COMPUTER SCIENCE, vol. 8425, p. 108-120, Springer Verlag, ISBN: 9783319068107, ISSN: 0302-9743, doi:10.1007/978-3-319-06811-4\_15
  - [86] S. Cimato, E. Damiani, R. Menicocci, and F. Zavatarelli, “Towards the certification of cloud services” in *IEEE 2013 International Workshop On Security and Privacy Engineering, Assurance, and Certification (SPEAC 2013)*, 2013 IEEE Ninth World Congress on Services (SERVICES 2013), page 100-105, Santa Clara, USA, June 2013. ISBN: 9780769550244, doi:10.1109/SERVICES.2013.16
  - [87] M. Sepehri, S. Cimato, and E. Damiani, “A Scalable Multi-Party Protocol for Privacy-Preserving Equality Test” in *International Workshop on Information Systems Security Engineering (WISSE 2013)*, CAiSE Workshops 2013, pp. 466-477, Valencia, Spain, June 2013. LECTURE NOTES IN BUSINESS INFORMATION PROCESSING, vol. 148, p. 466-477, Springer, ISBN: 9783642384899, ISSN: 1865-1348, Valencia, 2013, doi:10.1007/978-3-642-38490-5\_42
  - [88] S. Abbasi, S. Cimato, and E. Damiani, “Toward Secure Clustered Multi-Party Computation: A Privacy-Preserving Clustering Protocol”, in *Proceedings of ICT-EurAsia 2013*, LNCS 7804, pp. 447-452, Yogyakarta, Indonesia, 2013. ISBN: 9783642368172, doi:10.1007/978-3-642-36818-9\_49
  - [89] R. Tchokpon, S. Cimato and N. Bennani, “Ensuring XML Integrity using Watermarking Techniques”, in *Proceedings of 8th International Conference on Signal Image Technology & Internet Based Systems (SITIS 2012)*, IEEE Computer Society, Sorrento - Naples, Italy, 25-29, November 2012. ISBN: 9781467351522, doi:10.1109/SITIS.2012.101
  - [90] S. Cimato, Ching-Nung Yang and Chih-Cheng Wu, “Visual Cryptography based Watermarking: Definition and Meaning”, in *proceedings of 11th International Workshop on Digital forensics and Watermarking (IWDW 2012)*, LNCS 7809, 31 October- 3 November, Shanghai, China, 2012. ISBN: 9783642400988, doi:10.1007/978-3-642-40099-5\_36



- [91] C. Blundo and S. Cimato “Constrained Role Mining”, in *Proceedings 8th International Workshop on Security and Trust Management (STM 2012)* in conjunction with ESORICS 2012, LNCS 7783, Pisa, Italy - September 13-14, 2012. ISBN: 9783642380037 doi:10.1007/978-3-642-38004-4
- [92] M. Ali Hadavi, E. Damiani, R. Jalili, S. Cimato and Z. Ganjei, “AS5: A Secure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing”, in *proceedings of 5th International Workshop on Autonomous and Spontaneous Security (SETOP 2012)*, in conjunction with ESORICS 2012, LNCS 7731, Pisa, Italy - September 13-14, 2012. SPRINGER, ISBN: 9783642358890, Pisa, Italy, 2012, doi:10.1007/978-3-642-35890-6\_15
- [93] E. Damiani, S. Cimato, G. Gianini “Risk assessment of credit securities : the notion and the issues.”, in *Proceedings 6th IEEE International conference on digital ecosystems technologies - Complex environment engineering : IEEE (DEST-CEE 2012)*, Campione d’Italia. Campione d’Italia, Italy, June 18-20,2012. ISBN: 9781467317023, doi:10.1109/DEST.2012.6227954
- [94] M. Anisetti, E. Damiani, S. Cimato, F. Frati, G.Gianini, “Using Incentive Schemes to Alleviate Supply Chain Risks”, in *Proceedings of the International Conference on Management of Emergent Digital EcoSystems (MEDES)* , Bangkok, Thailand, October, 26-29, 2010. ISBN: 9781450300476, doi:10.1145/1936254.1936296
- [95] N. Bennani, S.Cimato and E. Damiani, “Toward cloud-based key management for outsourced databases”, in *Proceedings of the 2nd IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2010)*, Seoul, Korea, July 19-23, 2010. ISBN: 9781424480890, doi:10.1109/COMPSACW.2010.47
- [96] F. Benali, N. Bennani, G.Gianini and S.Cimato, “A Distributed and Privacy-preserving Method for Network Intrusion Detection”, in *Proceedings of the 12th International Symposium on Distributed Objects, Middleware, and Applications (DOA’10)*, Crete, Greece, October 26-29, 2010. ISBN: 9783642169489, doi:10.1007/978-3-642-16949-6\_13
- [97] C. Blundo, S. Cimato, “A Simple Role Mining Algorithm”, in *Proceedings of the 25th ACM Symposium on Applied Computing 2010. (SAC 2010)*, Crans-Montana, Switzerland, March 22-25, 2010. ISBN: 9781605586380, doi:10.1145/1774088.1774503
- [98] C. Blundo, S. Cimato, S. De Capitani Di Vimercati, A. De Santis, S. Foresti, S. Paraboschi, P. Samarati, “Efficient Key Management for Enforcing Access Control in Outsourced Scenarios”, in *Proceedings of the 24th IFIP TC-11 International Information Security Conference (SEC 2009)*. Cyprus, Greece, May 18-20, 2009. ISBN: 9783642012433, doi:10.1007/978-3-642-01244-0\_32
- [99] S. Cimato, E. Damiani and G. Gianini, “Privacy Preserving Risk Assessment of Credit Securities”, in *Proceedings of 5th International Conference on Signal Image Technology and Internet Based Systems (SITIS 09), Workshop on Security and Privacy in Telecommunication Systems (SePTIS)*, Marrakech, Morocco, 29-11, 2009. ISBN: 9781424457403
- [100] S. Cimato, M. Gamassi, V. Piuri, R. Sassi and F. Scotti , “Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System”, in *Proceedings of Annual Computer Security Applications Conference (ACSAC)*, Anaheim, California, USA, Dec. 8-12, 2008. ISBN: 9780769534473,

- [101] P. Ceravolo, S. Cimoto, F. Frati, C. Fugazza, E. Damiani, G. Gianini, S. Marrara, O. Scotti, “Hazards in Full-Disclosure Supply Chains”, in *Advanced Information Technologies for Management (AITM’2008)*, Ed. 35 di Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Jerzy Korczak, Helena Dudycz, Mirosław Dyczkowski Eds, Publishing House of the Wrocław University of Economics, Wrocław, Poland, 2008. ISSN 1899-3192
- [102] P. Ceravolo, S. Cimoto, E. Damiani, G. Gianini, C. Fugazza, S. Marrara “Risk Management and information Disclosure in Supply Chain Analysis”, in *Advanced Information Technologies for Management (AITM’2008)*, Ed. 35 di Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Jerzy Korczak, Helena Dudycz, Mirosław Dyczkowski Eds, Publishing House of the Wrocław University of Economics, Wrocław, Poland, 2008. ISSN 1899-3192
- [103] S. Cimoto, “A Lightweight Protocol for Dynamic RFID Identification”, in *3rd IEEE International Workshop on Security, Trust, and Privacy for Software Application(STPSA 2008) in conjunction with IEEE COMPSAC 2008*, Turku, Finland, IEEE Computer Press, July 2008. ISBN: 9780769532622
- [104] E. Damiani, P. Ceravolo, S. Cimoto, G. Gianini, “Obfuscation for the common good”, in *3rd conference on Security of Network Architectures and Information Systems (SAR/SSI 2008)*, Loctudy, Francia, Publibook, 2008. ISBN: 9782748343892
- [105] S. Cimoto, M. Gamassi, V. Piuri, R. Sassi and F. Scotti, “A multi-biometric verification system for the privacy protection of iris templates”, in *Proceedings of the second International Conference on Complex Intelligent and Software Intensive Systems (CISIS 2008)*, genova, Italy, Springer, September 2008. ISBN: 9783540881803,doi:10.1007/978-3-540-88181-0\_29
- [106] S. Cimoto, M. Gamassi, V. Piuri, R. Sassi and F. Scotti, “A biometric verification system addressing privacy concerns”, in *IEEE International Conference on Computational Intelligence and Security (CIS 2007)*, Harbin, China, December 2007, IEEE Computer Society Press, Washington USA, 2007. ISBN: 9780769530727
- [107] V. Auletta, C. Blundo, S. Cimoto, E. De Cristofaro and G. Raimato, “Authenticated Web Services: A WS-Security Based Implementation ”, in —em International Conference on New Technologies, Mobility and Security (NTMS’07), Paris, France, Kluwer Academic Publishers Group, The Netherlands, May 2007. ISBN: 978-1-4020-6269-8
- [108] S. Cimoto, M. Gamassi, V. Piuri, D. Sana, R. Sassi and F. Scotti, “Personal identification and verification using multimodal biometric data”, in *IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006)*, New York, IEEE Computer Society Press, USA, October 2006. ISBN: 1-4244-0745-1
- [109] V. Auletta, C. Blundo, S. Cimoto, and G. Raimato, “A Web Service Based Micro-payment System”, in —em Proceedings of IEEE Symposium on Computers and Communications (ISCC’06), Pula, Italia, IEEE Computer Society Press, Washington USA, Giugno 2006. ISBN: 0-7695-2588-1
- [110] S. Cimoto, C. Galdi, R. Giordano, B. Masucci and G. Tomasco, “Design and Implementation of a Certified Email Service”, in *Proceedings of 4th International Conference. on Cryptology and Network Security (CANS 2005)*, vol. 3810 di Lecture Notes in Computer Science, pp. 186-199, Xiamen, Cina, Springer Verlag Berlin Heidelberg, Germany, December 2005. ISBN: 3-540-30849-0

- [111] C. Blundo, S. Cimato and R. De Prisco, “A Lightweight Approach to Authenticated Web Caching”, in *Proceedings of 2005 International Symposium on Applications and the Internet (SAINT 2005)*, pp. 157–163, Trento, Italy, IEEE Computer Society Press, Washington, USA, January 2005. ISBN: 0-7695-2262-9
- [112] C. Blundo and S. Cimato, “A Framework for Authenticated Web Services”, in *Proceedings of European Conference on Web Services (ECOWS 04)*, vol. 3250 di Lecture Notes in Computer Science, pp. 61-71, Springer Verlag, Erfurt, Germany, September 2004. ISBN: 3-540-23202-8
- [113] S. Cimato, R. De Prisco and A. De Santis, “Colored Visual Cryptography without Color Darkening”, in *Proceedings of Fourth Conference on Security in Communication Networks '04 (SCN 04)*, vol. 3352 di Lecture Notes in Computer Science, pp. 235-248, Springer Verlag, Amalfi, Italy, September 2004. ISBN: 3-540-24301-1
- [114] V. Auletta, C. Blundo, S. Cimato and G. Raimato “A Web Service for Certified Email”, in *Proceedings of International Workshop on Certification and Security in Inter-Organizational E-Services (CSES 2004)*, Toulouse , France, Springer-IFIP, USA, August 2004. ISBN: 0-387-25087-5
- [115] C. Blundo and S. Cimato, “A Platform for Secure E-Gambling”, *Proceedings of the International Conference on Information Technology: Coding and Computing, (ITCC'04)*, pp.768-772 IEEE Computer Society Press, Washington USA, 2004. ISBN: 0-7695-2108-8
- [116] S. Cimato, P. D’Arco and I. Visconti, “Anonymous Group Communication in Mobile Networks”, *Proceedings of the 8th Italian Conference on Theoretical Computer Science, (ICTCS'03)*, vol. 2841 di Lecture Notes in Computer Science, pp. 316-328, Springer Verlag, 2003. ISBN: 3-540-20216-1
- [117] C. Blundo, S. Cimato and R. De Prisco, “Certified Email: Design and Implementation of a New Optimistic Protocol”, *Proceedings of the 8th IEEE Symposium on Computers and Communications (ISCC'03)*, pp. 828–833, IEEE Computer Society Press, Antalya, Turkey, 2003. ISBN: 0-7695-1961-X
- [118] S. Cimato, R. De Prisco and A. De Santis, “Contrast Optimal Colored Visual Cryptography Schemes”, *Proceedings of 2003 IEEE International Theory Workshop (ITW'03)*, pp. 139–142, IEEE, Paris, France, 31 March-4 April 2003. ISBN: 0-7803-7799-0
- [119] C. Blundo and S. Cimato, “SAWM: A Tool for Authenticated Web Metering”, *Proceedings 14th International Conference on Software Engineering and Knowledge Engineering (SEKE'02)*, pp. 641–648, ACM Press, New York, USA, 2002. ISBN: 1581135564
- [120] C. Blundo, S. Cimato and A. De Bonis, “A Lighthweight Protocol for the Generation and Distribution of Secure E-Coupons”, *Proceedings of the 11th World Wide Web Conference (WWW'02)*, pp. 542–552, ACM Press, Honolulu, Hawaii, USA 7-11 May 2002. ISBN: 1581134495
- [121] C. Blundo and S. Cimato, “Authenticated Metering”, *Poster Proceedings of the 11th World Wide Web Conference (WWW'02)*, ACM Press, Honolulu, Hawaii, USA 7-11 May 2002. ISBN: 1-880672-20-0
- [122] S. Cimato, “Design of an Authentication Protocol for GSM Javacards”, in *Proceedings of the 4th International Conference on Information Security and Cryptology (ICISC 2001)*, vol.

- 2288 di Lecture Notes in Computer Sciences, pp. 355–368, Springer Verlag, London, UK, 2001. ISBN: 3-540-43319-8
- [123] S. Cimoto and A. De Bonis, “Online Advertising: Secure E-Coupons”, *Proceedings of the 7th Italian Conference on Theoretical Computer Science (ICTCS’01)*, vol. 2202 di Lecture Notes in Computer Sciences, pp. 370–383, Springer Verlag, London, UK, 2001. ISBN: 3-540-42672-8
  - [124] S. Cimoto and P. Ciancarini, “A Formal Approach to the Specification of Java Components”, in *Workshop on Formal Techniques for Java Programs (ECOOP’99)*, Lisbon, Portugal, 1999. Appeared also in *Object-Oriented Technology, ECOOP’99 Workshop Reader, Workshops, Panels, and Posters*, vol. 1743 di Lecture Notes in Computer Sciences, pp. 107–108, Springer Verlag, London, UK, 1999. ISBN: 3-540-66954-X
  - [125] S. Cimoto, “Specifying Component-based Java Applications”, *Proceedings of the Third International Conference on Formal Methods for Open Object-Based Distributed Systems (FMOODS ’99)*, pp. 105–112, Kluwer Academic Publishers, The Netherlands, 1999. ISBN: ISBN 0-7923-8429-6
  - [126] P. Ciancarini and S. Cimoto, “Specifying Component-based Software Architectures”, *Workshop on Foundations of Component Based Systems (ESEC/FSE’97)*, pp. 60–70, 1997.
  - [127] S. Cimoto and C. Mascolo, “Analyzing and Animating Declarative Specifications”, *Proceedings of Joint Conference on Declarative Programming (APPIA-GULP-PRODE)*, M. Martelli and M. Navarro, Eds., pp.295-308, San Sebastian, Spain, 1996.
  - [128] P. Ciancarini and S. Cimoto, “Animating a Non-executable Formal Specification with a distributed symbolic language”, *Proceedings of the International Symposium on Design and Implementation of Symbolic Computation Systems (DISCO’96)*, vol. 1128 di Lecture Notes in Computer Science, pp. 200–201, Karlsruhe, Germany, September 18-20, 1996. ISBN 3-540-61697-7
  - [129] P. Ciancarini, S. Cimoto and C. Mascolo, “Engineering Formal Requirements: Analysis and Testing”, *Proceedings of 8th International Conference on Software Engineering and Knowledge Engineering (SEKE’96)*, pp. 385–392, Lake Tahoe, Nevada, USA, June 10-12, 1996. ISBN 0-9641699-3-2

## Brevetti

- [130] Cimoto S., Gamassi M., Piuri V., Sana D., Sassi R., Scotti F. “*Method for generating and verifying security information obtained by means of biometric readings*”, European patent no. WO2007113888, October, 2007
- [131] Cimoto S., Gamassi M., Piuri V., Sana D., Sassi R., Scotti F. “*Metodo di generazione e di verifica di una informazione di sicurezza ottenuta mediante letture biometriche* N. MI2006A000641. Università degli Studi di Milano. Domanda di brevetto depositata il 31 Marzo 2006.

## **Altre Pubblicazioni**

- [132] Fabio Scotti, S.Cimato and Roberto Sassi “Biometric Privacy” in *Encyclopedia of Cryptography and Security* (2nd Ed.) H.C.A. van Tilborg and S. Jajodia editors, Springer 2011: 101-104. ISBN: 9781441959058
- [133] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, F. Scotti, “Privacy Issues in Biometric Identification”, in *Information Security 2006*, Nigel Llyod ed., Touch Briefings, pp 40-42, 2006 ISBN:1-905052-96-0

## **6 Attività istituzionali, organizzative, di servizio, e di terza missione**

### **6.1 Attività istituzionali**

- Dal 2023 è membro della giunta esecutiva in qualità di rappresentante per Unimi della Fondazione ITS Nuove Tecnologie per il Made in Italy (Crema)
- Dal 2022 è rappresentante per il nodo di Milano presso il laboratorio nazionale CINI on Digital Skills, Training, Certifications
- Dal 2008 è membro e coordinatore del gruppo di ricerca per il tema ”Cybersecurity and Privacy” presso IRIXYS, Centro Internazionale di Ricerca e Innovazione in Sistemi Digitali Intelligenti nato dalla partnership di ricerca in Informatica tra l’Università di Passau, l’Institut National de Sciences Appliquées (INSA) di Lione, Università di Pau e l’Università degli Studi di Milano.

### **6.2 Attività di servizio per il Dipartimento e il Collegio Didattico**

- Da maggio 2023 è Co-responsabile della Commissione orientamento in ingresso del Dipartimento di Informatica
- Da maggio 2020 è referente AQ per il monitoraggio della qualità del Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche, Dipartimento di Informatica, Università degli Studi di Milano
- Da ottobre 2017 al maggio 2023 ha fatto parte della Giunta del Dipartimento di Informatica, Università degli Studi di Milano. in qualità di rappresentante eletto dei professori associati (e in conseguenza del Comitato di Direzione della Facoltà di Scienze e Tecnologie).
- Dal 2006 è membro della Commissione Tesi, Stage e Tirocini del Dipartimento di Informatica, Università degli Studi di Milano.
- Dal 2011 ad aprile 2023 è Membro della Commissione orientamento in ingresso del Dipartimento di Informatica
- Dal 2007 al 2011 è membro della commissione Orientamento Dipartimento di Tecnologie dell’Informazione/Informatica.

## **6.3 Attività di Terza Missione**

### **6.3.1 Organizzazione di stage a attività di orientamento per gli studenti di scuola superiore**

Per la commissione orientamento tiene/ha tenuto diversi seminari di orientamento

- In novembre 2024, ha svolto un ciclo di lezioni con tema Aspetti Tecnici e Informatici delle Criptovalute Titolo: “Blockchain e Sicurezza: Il Cuore Tecnologico delle Criptovalute” presso ITI Pino Hensemberger di Monza (MB). (10 ore)
- Dal 2020 al 2025 è responsabile per il Dipartimento di Informatica, dell’iniziativa Cyberchallenge, programma di addestramento in cybersecurity per studenti universitari e delle scuole superiori organizzato dal Cybersecurity National Lab, organizzando le selezioni locali e le lezioni (72 ore)
- Dal 2010 al 2024, ha tenuto seminari di Introduzione alla Crittografia durante la giornata Open Day (1 ora)
- Anni 2017 e 2019, stage di logica e problem solving per gli studenti delle scuole superiori (10 ore)
- Anni 2012-2015, Stage App-lichiamoci per gli studenti delle scuole superiori (15 ore)
- Anni 2012-2015, Stage App-lichiamoci2 per gli studenti delle scuole superiori (15 ore)
- Anno 2014, learning week presso l’istituto Volta di Lodi “APP- LINCHIAMOCI: un ambiente visuale per la promozione culturale” (25 ore).
- Anni 2012-2014, Stage Problem Solving per gli studenti delle scuole superiori (16 ore)
- Anni 2011-2014, Stage di preparazione per gli studenti delle scuole superiori per le Olimpiadi dell’Informatica (15 ore)

### **6.3.2 Attività di Public Engagement**

Attività di coinvolgimento e interazione con il mondo della scuola:

- (Organizzatore) - CRIPTOVALUTE LA RIVOLUZIONE MONETARIA E FINANZIARIA CHE STA CAMBIANDO IL MONDO Aula Magna, via Festa del Perdono, 7 (17/10/2023 )
- (Responsabile scientifico) - CRIPTOVALUTE: LA RIVOLUZIONE MONETARIA E FINANZIARIA CHE STA CAMBIANDO IL MONDO PROFILI GIURIDICO-ECONOMICI E TECNICO INFORMATICI PER UNA CONSAPEVOLE EDUCAZIONE FINANZIARIA Aula Magna via Festa del Perdono, 7 (19/05/2023)
- Altri eventi di pubblica utilità aperti alla comunità (Responsabile scientifico) - Evento Bookcity:Globalizzazione finanziaria e crisi economiche. Uno scenario a fasi alternate tra forte interconnessione e minore intensità Aula Crociera, Dipartimento di Giurisprudenza in Via Festa del Perdono (17/11/2022)
- Altre iniziative di Public Engagement (Relatore) - Conversazioni digitali. Quanto e come digitale e tecnologia sono entrati nella nostra vita quotidiana. Dipartimento di Informatica Giovanni Degli Antoni Biblioteca Comunale ”Clara Gallini” - Sala conferenze (17/10/2017)
- Dal 2012 al 2014 ha organizzato e tenuto un Ciclo di lezioni di “Introduzione alla didattica con l’Ipad” destinate ai docenti della scuola d’infanzia e primaria del plesso di Cremauno di Crema

Milano, 10 Gennaio 2025