Ivan Visconti

Curriculum Vitae - ai fini della pubblicazione

Luogo: Salerno
Data: 13 Dicembre 2023

Parte I - Informazioni Generali

Nome e Cognome: Ivan Visconti
Data di Nascita:
Luogo di Nascita:
Cittadinanza:
Indirizzo di Residenza:
Telefono:
E-mail:
Conoscenza delle Lingue: Italiano (madrelingua), Inglese (fluente)

Parte II - Studi

- Ottobre 1998: Conseguimento della laurea in informatica (5 anni) 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.
- 1999 - 2002: Studente di dottorato di ricerca in Informatica dell'Università di Salerno. Concorso vinto classificandosi al primo posto.
- 2003 (Febbraio): Conseguimento del titolo di *Dottore di Ricerca in Informatica* presso l'Università di Salerno.
  Tesi : On Authentication and Privacy on the Internet.
  Tutor : Prof. Giuseppe Persiano.
  Coordinatore : Prof. Alfredo De Santis.

Part III - Posizioni lavorative, Abilitazioni, Visite di ricerca, Attività in collegi/commissioni

Posizioni lavorative

Dal 2019: Professore ordinario di Informatica (01/B1), Università di Salerno (L240/2010).
Dal 2014 al 2019: Professore associato di Informatica (01/B1), Università di Salerno (L240/2010).
Dal 2005 al 2014: Ricercatore universitario di Informatica (SSD INF/01 - Informatica), Università di Salerno.
Dal 2003 al 2004: Ricercatore Post-Doc per 12 mesi presso il "Complexity and Cryptography Research Group" di ENS Parigi, Francia.

- Dal 01/12/2004 al 31/10/2005 (11 mesi): Titolare di un assegno di ricerca denominato "Criptologia" presso il Dipartimento di Informatica ed Applicazioni - Università di Salerno.
- Dal 01/10/1999 al 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.

Abilitazioni

- Da Aprile 2017 abilitato ASN alla I fascia per il settore concorsuale 01/B1 Informatica.
- Dal 2014 abilitato ASN alla II fascia per il settore concorsuale 01/B1 Informatica.

Partecipazione a collegi di dottorato

- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INFORMATICA" Anno accademico di inizio: 2008 - Ciclo: XXIV - Durata: 3 anni
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "TEORIE,METODOLOGIE E APPLICAZIONI AVANZATE PER LA COMUNICAZIONE,L'INFORMATICA E LA FISICA" Anno accademico di inizio: 2009/10 - Ciclo: XXV - Durata: 3 anni
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INFORMATICA" Anno accademico di inizio: 2010/11 - Ciclo: XXVI - Durata: 3 anni
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INFORMATICA" Anno accademico di inizio: 2011/12 - Ciclo: XXVII - Durata: 3 anni
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INFORMATICA" Anno accademico di inizio: 2012/13 - Ciclo: XXVIII - Durata: 3 anni
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INFORMATICA E INGEGNERIA DELL'INFORMAZIONE" Anno accademico di inizio: 2013/14 - Ciclo: XXIX - Durata: 3 anni dal 01-11-2013 al 31-10-2016
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INFORMATICA E INGEGNERIA DELL'INFORMAZIONE" Anno accademico di inizio: 2014/15 - Ciclo: XXX - Durata: 3 anni
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "MANAGEMENT & INFORMATION TECHNOLOGY" Anno accademico di inizio: 2015/16 - Ciclo: XXXI - Durata: 3 anni
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "MANAGEMENT & INFORMATION TECHNOLOGY" Anno accademico di inizio: 2016/17 - Ciclo: XXXII
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INGEGNERIA DELL'INFORMAZIONE" Anno accademico di inizio: 2018/19 - Ciclo: XXXIV
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INGEGNERIA DELL'INFORMAZIONE" Anno accademico di inizio: 2019/20 - Ciclo: XXXV
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INGEGNERIA DELL'INFORMAZIONE" Anno accademico di inizio: 2020/21 - Ciclo: XXXVI
- Ateneo proponente: Università degli Studi di SALERNO Titolo: "INGEGNERIA DELL'INFORMAZIONE" Anno accademico di inizio: 2021/22 - Ciclo: XXXVII

Partecipazione a commissioni

- Membro della "commissione paritetica docenti-studenti" per 5 anni, presso il DIEM, Università di Salerno, e di vari altre commissioni ("Test D'Ingresso", "Assegnazione Spazi" e "WEB") nel precedente dipartimento (DI).
- Membro delle commissione per la selezioni di due ricercatori RTDA all'Università Roma Tre e di un ricercatore RTDA all'Università di Trento.
- Membro delle commissioni in relazione alla valutazione del conseguiemnto del titolo di dottore di ricerca dei seguenti candidati: Marco Zecchini (Università La Sapienza), Orazio Puglisi (Università di Catania), Prastudy Fauzi (University of Tartu), Najmeh Soroush (University of Luxembourg), Chan Nam Ngo (Università di Trento).
- Membro in più occasioni di commissioni per l'aggiudicamento di assegni di ricerca, di borse di studio, di contratti per il supporto alla didattica, di contratti di insegnamento dell'Università di Salerno.
- Membro di una commissione per un bando del dottorato di ricerca in Informatica ed Ingegneria dell'Informazione dell'Università di Salerno.
- Valutatore di progetti relativi a vari bandi nazionali e internazionali quali Futuro in Ricerca 2010, "Innovational Research Incentives Scheme" del "Division for Physical Sciences of the Netherlands Organisation for Scientific Research" 2010, Israel Science Foundation 2016, FIL 2016 Incentivising Quota dell'Università di Parma 2016, Excellence programme of the Vienna Science and Technology Fund WWTF 2018.

Visite di ricerca di lungo periodo

1. Computer Science Department of UCLA, Los Angeles, California, ospitato dal prof. Rafail Ostrovsky per circa 1 anno nel 2015/2016, circa 2 anni nel 2010/2012, circa 6 mesi nel 2009/2010.
2. IBM Zurich Research Lab., circa 4 mesi, 2002, Svizzera, ospitato dal by Dr. Christian Cachin.

Principali visite di ricerca di breve periodo

1. Agosto 2023, in visita per circa una settimana su invito del prof. Georg Fuchsbauer presso il Security and Privacy group di TU Wien, Vienna, Austria.
2. Gennaio 2023, in visita per circa una settimana su invito dei proff. Daniele Venturi e Andrea Vitaletti presso l'Università la Sapienza di Roma.
3. Ottobre 2016: In visita per circa una settimana su invito del prof. Sanjam Garg, al computer science department di University of Berkeley (UCB), USA.
4. Febbraio 2014 - In visita per circa 3 settimane su invito del prof. Rafail Ostrovsky presso UCLA, Los Angeles, USA.
5. Ottobre-Novembre 2013 - In visita per circa 5 settimane su invito del prof. Rafail Ostrovsky presso UCLA, Los Angeles, USA.
6. Febbraio 2013 - In visita per circa 3 settimane presso UCLA, su invito del prof. Rafail Ostrovsky Los Angeles, USA.
7. Giugno 2012 - In visita per circa una settimana presso il Microsoft Research Center, su invito della Dott.ssa Melissa Chase Redmond, USA.

8. Agosto 2010 - In visita per circa una settimana su invito del prof. Ahmad-Reza Sadeghi presso il System Security Group, Horst Görtz Institute for IT-Security, Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germania.
9. Febbraio 2010 - In visita per circa una settimana su invito del prof. Ahmad-Reza Sadeghi presso il System Security Group, Horst Görtz Institute for IT-Security, Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germania.
10. Dicembre 2008 - In visita per circa due settimane su invito del prof. Ahmad-Reza Sadeghi presso il System Security Group, Horst Görtz Institute for IT-Security, Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germania.
11. Novembre 2008 - In visita per circa una settimana su invito del Dott. Seny Kamara presso il Microsoft Research Center, Redmond, USA.
12. Febbraio 2008 - In visita per circa una settimana su invito del prof. Ahmad-Reza Sadeghi presso il System Security Group, Horst Görtz Institute for IT-Security, Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germania.
13. Novembre 2006: Partecipazione per circa 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, USA.

Part IV – Attività Didattiche

Didattica per studenti di dottorato e in international schools:

1. "Crypto and Incentive-Based Mechanisms for Blockchain Technology", 12 ore, per il dottorato di ricerca in Data Science dell'Università La Sapienza (2023).
(`https://www.diag.uniroma1.it/node/27187`)
2. Insegnamento di un corso di 10 ore denominato "Security Notions for Secure Computation" per gli studenti del Dottorato di Ricerca in Informatica ed Ingegneria dell'Informazione dell'Università di Salerno, nel 2014.
(`http://www.di-srv.unisa.it/professori/ads/PhD/Dottorato_di_Ricerca/Corsi_2014.html`)
3. Relatore alla ECRYPT II PhD Summer School on Applied Cryptographic Protocols svoltasi a Mykonos, Grecia, presentando due lezioni dal titolo "Identification Schemes I" e "Identification Schemes II", nel 2010.
(`https://www.ecrypt.eu.org/ecrypt2/webnews/webnews0111.htm`)
4. 2022 Relatore alla Algorand school on "Blockchain consensus mechanisms", per tre ore e trenta minutiper l' on-line School on Algorand Smart Contracts (https://algorandschool.github.io/algorand-school/)

Didattica per studenti di corsi di laurea e laurea magistrale/specialistica:

- Anno accademico 2023/2024: Algoritmi e Strutture Dati - 6 CFU, laurea in Ingegneria Informatica, Università di Salerno (in corso).
- Anno accademico 2022/2023: Algoritmi e Protocolli per la Sicurezza - laurea magistrale in Ingegneria Informatica, corso erogato per 2 volte per un totale di 18 CFU, Università di

Salerno.

- Anno accademico 2022/2023: Algoritmi e Strutture Dati - 6 CFU, laurea in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2021/2022: Algoritmi e Protocolli per la Sicurezza - laurea magistrale in Ingegneria Informatica, corso erogato per 2 volte per un totale di 12 CFU, Università di Salerno.
- Anno accademico 2021/2022: Algoritmi e Strutture Dati - 6 CFU, laurea in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2020/2021: Cybersecurity - laurea magistrale in Ingegneria Informatica, corso erogato per 2 volte per un totale di 10 CFU, Università di Salerno.
- Anno accademico 2020/2021: Algoritmi e Strutture Dati - 6 CFU, laurea in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2019/2020: Cybersecurity - laurea magistrale in Ingegneria Informatica, corso erogato per 2 volte per un totale di 9 CFU, Università di Salerno.
- Anno accademico 2019/2020: Algoritmi e Strutture Dati - 48 ore - Bachelor, 6 CFU, laurea in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2018/2019: Architettura dei calcolatori e sistemi operativi, 6 CFU, laurea in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2018/2019: Laboratorio di Programmazione, 6 CFU, laurea in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2018/2019: Sicurezza Informatica, 3 CFU, laurea magistrale in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2017/2018: Laboratorio di Programmazione, 3 CFU, laurea in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2017/2018: Secure Protocols and Primitives for Computation and Communication, 10 CFU, laurea magistrale in Business, Innovazione ed Informatica, Università di Salerno.
- Anno accademico 2017/2018: Architettura dei calcolatori e sistemi operativi, 6 CFU, laurea in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2016/2017: Secure Protocols and Primitives for Computation and Communication, 10 CFU, laurea magistrale in Business, Innovazione ed Informatica, Università di Salerno.
- Anno accademico 2016/2017: Laboratorio di Programmazione, 6 CFU (48 ore), laurea triennale in Ingegneria Informatica, Università di Salerno.
- Anno accademico 2014/2015: Programmazione I (modulo II - 6 CFU, laurea triennale in Informatica, Università di Salerno).
- Anno accademico 2014/2015: Programmazione Sicura (2 CFU, laurea magistrale in Informatica, Università di Salerno).
- Anni accademici 2012/2013 - 2013/2014 - 2014/2015: Strutture Dati (6 CFU, laurea triennale in Informatica, Università di Salerno).
- Anno accademico 2009/2010 - Corso di Recupero di Lab. di Sistemi Operativi (laurea triennale in Informatica, Università di Salerno).

- Anni accademici 2005/2006 - 2006/2007 - 2007/2008 - 2008/2009: Lab. di Sistemi Operativi (laurea triennale in Informatica, Università di Salerno).
- Anno accademico 2006/2007: Lab. di Crittografia e Sicurezza dell'Informazione (laurea specialistica in Informatica, Università di Salerno).
- Anni accademici 2007/2008 - 2008/2009: Strumenti di Crittografia per la Sicurezza dell'Informazione (laurea specialistica in Informatica, Università di Salerno).
- Anno accademico 2007/2008: Sicurezza su Reti (laurea triennale in Informatica, Università di Salerno).
- 2005-2023: Relatore di oltre 20 tesi per la laurea triennale in informatica, di oltre 15 tesi tra laurea in informatica (vecchio ordinamento), laurea specialistica/magistrale in informatica e laurea magistrale in ingegneria informatica all'Università di Salerno.
- 2005-2023: Attività di tutor per oltre 20 tirocini relativi alle laurea in informatica e ingegneria informatica all'Università di Salerno.
- Partecipazione alle attività del programma ERASMUS dell'Università di Salerno, in qualità di coordinatore degli accordi con l'Università di Bochum (Germania), di Tartu (Estonia) e di Erlagen-Norimberga (Germania).

Part V - Affiliazione ad associazioni, Premi e Riconoscimenti

1. Ricevuto il best paper award per la pubblicazione nella 21st International Conference on Cryptology and Network Security - CANS 2022 - `https://www.youtube.com/watch?v=lFGa7Hc3GVc&t=449s`, autori della pubblicazione premiata: Michele Ciampi e Ivan Visconti.
2. Ricevuto da IEEE il Certificate of Merit "for outstanding editorial board service for the IEEE Transactions on Information Forensics and Security", 2020.
3. Ricevuto da IEEE il Certificate of Appretiation "in recognition of service as Senior Area Editor of IEEE Transactions on Information Forensics and Security", 2022.
4. Ottenimento di un finanziamento dalla provincia di Salerno nell'ambito di un programma a supporto della mobilità internazionale dei giovani ricercatori coordinato dall'Università di Salerno; il grant ha supportato la visita di 6 mesi presso UCLA (USA) da Agosto 2009 a Gennaio 2010.
5. Relatore della tesi dottorato di Alessandra Scafuro (2009-2012) che ha ricevuto l'award per best PhD thesis in theoretical computer science in Italy (Italian Chapter, EATCS).
6. Relatore della tesi dottorato di Luisa Siniscalchi (2014-2017) che ha ricevuto l'award per best PhD thesis in theoretical computer science in Italy (Italian Chapter, EATCS).
7. Management Committee Member per l'Italia dell'ICT COST Action IC1306 "Cryptography for Secure Digital Interaction" (2014-2018).
8. Dal 2019 Membro dell'academic advisory body dell'International Association for Trusted Blockchain Applications (INATBA).
   `https://inatba.org/aab-members/`
9. Affiliato alle associazioni ACM, IEEE, EATCS, IACR, GNCS.

Parte VI - Progetti finanziati in qualità di responsabile scientifico, Partecipazioni a progetti finanziati e Trasferimento tecnologico

Progetti finanziati con ruolo di responsabile scientifico e conseguente coordinamento del gruppo di ricerca:

- **EU H2020 RIA**: Responsabile scientifico per l'università di Salerno del progetto "Privacy-enhancing cryptography in distributed ledgers" (PRIViLEDGE) con un finanziamento di oltre 445.000,00 euro per il periodo 2018-2021.
  (`https://docenti.unisa.it/004312/ricerca/progetti?progetto=32514`)
- **IT MIUR PRIN**: Responsabile scientifico per l'università di Salerno del progetto PRIN2022 "PrepAring cRypTograpHy for privacy-awarE blockchaiN applicatiONs (PARTHENON)" finanziato con oltre 50.000,00 euro, 2023-2026.
  (`https://docenti.unisa.it/004312/ricerca/progetti?progetto=60523`)
- Responsabile per circa 1 anno del progetto di ricerca scientifica "Sicurezza dell'Informazione e Reti Sociali: Modelli, Algoritmi e Applicazioni" 2014-2016 finanziato con fondi di Ateneo per la Ricerca di Base (FARB) dall'Università di Salerno, per 20.131,10 euro. Dopo circa un anno il ruolo di responsabile è stato lasciato a causa del congedo per motivi di studio.
- Responsabile del progetto di ricerca scientifica "TEORIA ED APPLICAZIONI DELLA CRITTOGRAFIA MODERNA, DELLE RETI DI COMUNICAZIONE E DELLE RETI SOCIALI" 2015-2017 finanziato con fondi di Ateneo per la Ricerca di Base (FARB) dall'Università di Salerno, per 19.236,99 euro.
  `https://docenti.unisa.it/004312/ricerca/progetti?progetto=24882`
- Responsabile del progetto di ricerca scientifica "STUDIO DELLA PROTEZIONE DEI DATI NEL CYBERSPACE MEDIANTE TECNICHE AVANZATE DI CRITTOGRAFIA E DI DECENTRALIZZAZIONE" 2022-2025 finanziato con fondi di Ateneo per la Ricerca di Base (FARB) dall'Università di Salerno, per 7.970,00 euro.
  `https://docenti.unisa.it/004312/ricerca/progetti?progetto=50343`
- Responsabile del progetto di ricerca scientifica "CRITTOGRAFIA MODERNA E BLOCKCHAIN" 2023-2026 finanziato con fondi di Ateneo per la Ricerca di Base (FARB) dall'Università di Salerno, per 4.283,00 euro.
  `https://docenti.unisa.it/004312/ricerca/progetti?progetto=59063`
- Responsabile scientifico del progetto nazionale initolato "Costruzioni Avanzate di Sigma-Protocols e Applicazioni" finanziato da GNCS-INDAM (Gruppo Nazionale per il Calcolo Scientifico, ISTITUTO NAZIONALE DI ALTA MATEMATICA "F. SEVERI") con 3.000 euro.
  (`https://docenti.unisa.it/004312/ricerca/progetti?progetto=26155`)

Partecipazione a progetti finanziati

- Partecipazione alle attività di ricerca dei gruppi denominati Asymmetric Techniques Virtual Lab (AZTEC) e Protocols Virtual Lab (PROVILAB) e parte del Network of Excellence "ECRYPT" (commissione europea, sesto programma quadro, 2004-2008).
- Partecipazione alle attività di ricerca dei gruppi di ricerca denominati Multi-party and Asymmetric Algorithms Virtual Lab (MaYA) e Symmetric Techniques Virtual Lab (SymLAB) e parte del Network of Excellence "ECRYPT 2" (commissione europea, settimo programma quadro, 2008-2013).

- Partecipazione alle attività di ricerca su "Adapting the Network Infrastructure" dello Specific targeted research project (STREP) denominato "Foundations of Adaptive Networked Societies of Tiny Artefacts (Fronts)" (commissione europea, settimo programma quadro, 2008-2011).
- Partecipazione alle attività di ricerca su "Security and Trust Management" dell'IST FET Integrated Project "Algorithmic Principles for Building Efficient Overlay Computers (AEOLUS)" (commissione europea, sesto programma quadro, 2005-2009).
- Partecipazione alle attività di ricerca dei seguenti progetti FARB (Finanziamenti alla Ricerca di Base) finanziati dall'Università di Salerno: a) 2006-2008 "Sicurezza delle reti, animazione di protocolli crittografici e algoritmi". b) 2007-2009 "Modelli Algoritmici per Agenti Egoisti e Maliziosi". c) 2008-2010 "Modelli Algoritmici per Agenti Egoisti e Maliziosi". d) 2009-2011 "Modelli Algoritmici per Agenti Egoisti e Maliziosi". e) 2010-2012 "Privacy e trust". f) 2011-2013 "Modelli Algoritmici per Agenti Privati e Fidati". g) 2012-2014 "Crittografia e Teoria dei Giochi". h) 2013-2015 "Modelli, Teoria dei Giochi e Crittografia". k) 2016-2018 "Estrazione, comprensione e gestione della informazione e del ruolo dei membri nelle reti sociali."
- Partecipazione al progetto "Smart Tunnel - piattaforma intelligente servizi logistici per le città portuali, PON "Ricerca e Competitività 2007/2013" Asse II, (Codice: PON 04a2 G), dal 2012 al 2015.
- Partecipazione al progetto "MyOpenGov" POR Campania FESR 2007-2013, dal 2013 al 2015
- Partecipazione al progetto di ricerca "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), 2009-2010.
- Partecipazione al Programmi di Ricerca Scientifica di Rilevante Interesse Nazionale (PRIN) intitolato "Progettazione ed analisi di protocolli crittografici per la tutela della privacy personale e dei dati in basi di dati e dispositivi mobili", 2008-2010.
- Partecipazione al progetto di ricerca intitolato "Protocolli Efficienti per il Two Party Secure Text-Processing", finanziato dal GNCS-INDAM (Gruppo Nazionale per il Calcolo Scientifico, ISTITUTO NAZIONALE DI ALTA MATEMATICA "F. SEVERI"), nel 2011.
- Partecipazione al progetto di ricerca intitolato "Strumenti Algoritmici e Crittografici per l'Elaborazione, il Mantenimento e la Trasmissione di Dati su Server Remoti", finanziato dal GNCS-INDAM (Gruppo Nazionale per il Calcolo Scientifico, ISTITUTO NAZIONALE E DI ALTA MATEMATICA "F. SEVERI"), nel 2012.
- Partecipazione al Programmi di Ricerca Scientifica di Rilevante Interesse Nazionale (PRIN) intitolato "Data-Centric Genomic Computing (GenData 2020)", 2013-2016.
- Partecipazione al progetto intitolato "Privacy e Sicurezza in Online Social Networks" finanziato da GNCS-INDAM (Gruppo Nazionale per il Calcolo Scientifico, ISTITUTO NAZIONALE DI ALTA MATEMATICA "F. SEVERI") nel 2017.

Trasferimento tecnologico

- 2001 - Partecipazione con retribuzione alla convenzione di ricerca ex. Art. 66 dl 382/80 tra il Dipartimento di Informatica ed Applicazioni dell'Università di Salerno e l'azienda E-CNET

(importo delle convenzione: 100.000.000 di Lire), contribuendo al ridisegno architetturale di una piattaforma per il commercio elettronico con prerogative estremamente originali.

- 2001-2002 - Partecipazione con retribuzione ad una convenzione di ricerca ex. Art. 66 dl 382/80 tra il Dipartimento di Informatica ed Applicazioni dell'Università di Salerno e l'azienda STT spa (importo della convenzione: per un importo di 130.000.000 di Lire), contribuendo all'analisi delle prestazioni e l'ottimizzazione della piattaforma sviluppata in collaborazione con E-CNET in condizione di esercizi.
- 2006-2007 - Partecipazione con retribuzione alla convenzione di ricerca ex. Art. 66 dl 382/80 tra il Dipartimento di Informatica ed Applicazioni dell'Università di Salerno e l'azienda Bit4ID S.r.l. (importo della convenzione: 107.000 Euro), contribuendo allo sviluppo di una serie di moduli per l'autenticazione e la firma digitale per una network appliance dedicata (Hardware Security Module).
- 2018 - Partecipazione con retribuzione alla convenzione DIEM - CONSORZIO CONSEL relativa a corsi avanzati presso l'azienda ERICSSON di Pagani.
- Responsabile dell'accordo quadro tra il DIEM dell'Università di Salerno e Farzati Tech Srl per l'utilizzo delle blockchain applicate alla tracciabilità della filiera agroalimentare. Nell'ambito di questo accordo, Farzati Tech Srl ha finanziato una borsa di studio per attività di ricerca semestrale. (`https://www.diem.unisa.it/ricerca/progetti-finanziati?progetto=41247`)

Parte VII – Attività di Ricerca

Il crescente utilizzo/sfruttamento dei dati ed il loro ruolo nelle piattaforme digitali amplifica i rischi di possibili abusi in vari contesti del Cyberspace. Malgrado gli impressionanti progressi della ricerca sulle tecniche crittografiche per la protezione dei dati, restano limitate le funzionalità che possono essere realizzate in modo robusto utilizzando unicamente strumenti standardizzati. La conseguente necessità di utilizzare anche strumenti non ancora standardizzati incrementa la domanda di esperti in grado di progettare, analizzare ed utilizzare strumenti avanzati di crittografia per la Cybersecurity.

La mia ricerca in Cybersecurity è orientata al risolvere problemi aperti legati alla sicurezza dei dati e la loro confidenzialità. L'obiettivo della mia ricerca è fornire strumenti e tecniche per la protezione dei dati con lo scopo di consentire la costruzione di sistemi digitali in grado di garantire data security e privacy by design. Il punto di forza della mia ricerca è la conoscenza avanzata della crittografia moderna che include nozioni e tecniche sofisticate che, opportunamente migliorate ed adattate ai contesti di riferimento, consentono la realizzazione di servizi fault-tolerant incentrati sul concetto del garantire la sicurezza dei dati *in uso*.

La mia ricerca include due direzioni principali. La prima consiste in un'analisi critica dei sistemi noti con l'obiettivo di identificare debolezze dei modelli e delle assunzioni sui quali sono stati costruiti, espondendo quindi possibili vulnerabilità. La seconda consiste nel progettare soluzioni alternative focalizzate sui noti principi di security e privacy by design, ma anche sul più recente principio del garantire decentralizzazione by design, mitigando le vulnerabilità legate al single point of failure. Molti dei miei risultati di ricerca sono stati presentati nelle conferenze più importanti di crittografia a livello mondiale ed sono stato invitato molte volte a partecipare ai comitati di programma di tali conferenze. E' mia intenzione orientare ulteriormente la mia ricerca verso

la costruzione del ponte tra teoria e pratica in modo da contribuire a sviluppare e rendere fruibili tecniche utili a garantire la sicurezza dei sistemi che utilizzano dati confidenziali di individui e organizzazioni.

Tra gli scenari più rilevanti in Cybersecurity c'è il crescente sviluppo di sistemi che utilizzano tecniche di Intelligenza Artificiale. Quest'ultima è sempre più usata sia per rafforzare meccanismi di attacco (es. identificando nuove vulnerabilità da sfruttare) sia per rafforzare meccanismi di difesa (es. identificando contromisure ad attacchi). Al tempo stesso, le tecniche di AI possono esporre nuove vulnerabilità legate all'integrità e la confidenzialità dei dati coinvolti. La mia ricerca in tale contesto è orientata alla protezione dei dati coinvolti nei sistemi basati su AI, e a rendere tali sistemi trasparenti, robusti ed equi.

Principali attività in comitati di programma, editorial boards e di reviewer esterno

1. **Program Co-Chair** di "5th Distributed Ledger Technology Workshop (DLT 2023)", Bologna, May 2023, CEUR-WS.
   (`https://dltgroup.dmi.unipg.it/DLTWorkshop/dlt2023.html`)
2. Dal 2019 al 2021, Senior Area Editor of IEEE Transactions on Information Forensics and Security (**T-IFS**).
3. Da Giugno 2017 al 2021 associate editor della rivista "IEEE Transactions on Information Forensics and Security".
4. **Program Co-Chair** di "Workshop on Privacy ENhancing Cryptography In Ledgers" (PENCIL 2019)", Darmstadt, May 2019
   (`https://eurocrypt.iacr.org/2019/affiliatedevents.html`)
5. **Program Chair** di "The 8th Conference on Security and Cryptography for Networks (SCN 2012)" - *LNCS Springer-Verlag*, Amalfi, September 2012.
6. Membro del Program Committee di "The 43rd Advances in Cryptology (EUROCRYPT 2024)" - **IACR** - *LNCS Springer-Verlag.*
7. Membro del Program Committee di "The 26th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2023)" - **IACR** - *LNCS Springer-Verlag.*
8. Membro del Program Committee di "The 41st Advances in Cryptology (EUROCRYPT 2022)" - **IACR** - *LNCS Springer-Verlag.*
9. Membro del Program Committee di "The 27th European Symposium on Research in Computer Security (ESORICS 2022)" - *LNCS Springer-Verlag.*
10. Membro del Program Committee di "The 20th International Conference on Applied Cryptography and Network Security (ACNS 2022)" - *LNCS Springer-Verlag.*
11. Membro del Program Committee di "The 59th Annual IEEE Symposium on Foundations of Computer Science (**FOCS 2018**)" - **IEEE**.
12. Membro del Program Committee di "The 15th IACR Theory of Cryptography Conference (TCC 2018)" - **IACR** - *LNCS Springer-Verlag.*
13. Membro del Program Committee di "The 37th Advances in Cryptology (EUROCRYPT 2018)" - **IACR** - *LNCS Springer-Verlag.*
14. Membro del Program Committee di "The 16th International Conference on Applied Cryptography and Network Security (ACNS 2018)" - *LNCS Springer-Verlag.*
15. Membro del Program Committee di "The 23rd Conference on the Theory and Application

of Cryptology and Information Security (ASIACRYPT 2017)" - **IACR** - *LNCS Springer-Verlag.*

16. Membro del Program Committee di "The 20th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2017)" - **IACR** - *LNCS Springer-Verlag.*
17. Membro del Program Committee di "The 15th International Conference on Applied Cryptography and Network Security (ACNS 2017)" - *LNCS Springer-Verlag.*
18. Membro del Program Committee di "The 35th Advances in Cryptology (EUROCRYPT 2016)" - **IACR** - *LNCS Springer-Verlag.*
19. Membro del Program Committee di "The 22nd Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2016)" - **IACR** - *LNCS Springer-Verlag.*
20. Membro del Program Committee di "The 14th International Conference on Applied Cryptography and Network Security (ACNS 2016)" - London, UK - *LNCS Springer-Verlag.*
21. Membro del Program Committee di "The 13th IACR Theory of Cryptography Conference (TCC 2016)" - **IACR** - *LNCS Springer-Verlag.*
22. Membro del Program Committee di "The 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2015 - Track A)" - **EATCS** - *LNCS Springer-Verlag.*
23. Membro del Program Committee di "The 34th Cryptology Conference (CRYPTO 2014)" - **IACR** - *LNCS Springer-Verlag.*
24. Membro del Program Committee di "The 33rd Advances in Cryptology (EUROCRYPT 2014)" - **IACR** - *LNCS Springer-Verlag.*
25. Membro del Program Committee di "The 31st Advances in Cryptology (EUROCRYPT 2012)" - **IACR** - *LNCS Springer-Verlag.*
26. Membro del Program Committee di "The 15th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2012)" - **IACR** - *LNCS Springer-Verlag.*
27. Membro del Program Committee di "The 9th International Conference on Applied Cryptography and Network Security (ACNS 2011)" - Malaga, Spain. - *LNCS Springer-Verlag.*
28. Membro del Program Committee di "The 13th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2010)" - **IACR** - *LNCS Springer-Verlag.*
29. Membro del Program Committee di "The 15th Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2009)" - **IACR** - *LNCS Springer-Verlag.*
30. Membro del Program Committee di "The 12th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2009)" - **IACR** - *LNCS Springer-Verlag.*
31. In qualità di reviewer esterno, il sottoscritto ha svolto review per Journal of ACM, Journal of Computer and System Sciences, SIAM Journal on Computing.

Presentazioni su invito (in presenza)

1. 16th International Conference on Security for Information Technology and Communications (SECITC 2023), Bucharest (Romania), 2023.
   (`https://secitc.eu/`)
2. CROSSING Conference 2023, Darmstadt, Germany.

(https://www.crossing.tu-darmstadt.de/news_events/conferences_workshops/crossing_conference_2023/crossing_conference_2023_speakers.en.jsp)

3. 3rd Distributed Ledger Technology (DLT 2020), Tutorial, "Data Privacy in Blockchains: Theory and Practice", Ancona, Italy, 2020.
   (https://2020.itasec.it/ITASEC20/data-privacy-in-blockchains-theory-and-practice-tutorial/)
4. Riunione annuale GTTI, "Tutorial Blockchain", Pavia, Italia, 2019.
   (https://www.gtti.it/eventi-gtti/riunioni-annuali/riunione-annuale-2019-programma/)
   (https://2020.itasec.it/ITASEC20/data-privacy-in-blockchains-theory-and-practice-tutorial/)
5. 17th International Conference on Cryptology And Network Security (CANS 2018), Naples, Italy, 2018.
   (https://cans2018.na.icar.cnr.it/guestspeakers.html)
6. 4th International Forum on Research and Technologies for Society and Industry (IEEE RTSI), Palermo, Italy, 2018.
   (https://rtsi2018.ieeesezioneitalia.it/technical_program.html)
7. 13th conference on Computability in Europe (CIE), Turku, Finland, 2017.
   (https://math.utu.fi/cie2017/schedule/)
8. STAR (Seminar on Theory, Algorithms and cRyptography Research) seminar at UCSD (Novembre 2009, La Jolla - CAL - USA), 2009, invitato dal prof. Daniele Micciancio.
9. Distinguished Lecturer Seminar Series at UCI (Novembre 2009, Irvine - CAL - USA), 2009, invitato dai prof. Gene Tsudik e Stas Jarecki.
10. Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference II (Giugno 2009, Lake Arrowhead - CAL - USA).
11. Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security: Reunion Conference I (Giugno 2008, Lake Arrowhead - CAL - USA).
12. Workshop on Foundations of Secure Multi-Party Computation and Zero-Knowledge (Nov. 2006, Los Angeles - USA).
    https://www.ipam.ucla.edu/programs/workshops/workshop-iii-foundations-of-secure-multi-party-computation-and-zero-knowledge-and-its-applications/?tab=speaker-list
13. Workshop on Security Hardware in Theory and Practice: A Marriage of Convenience, Dagstuhl, Germany, 2008.
    https://www.dagstuhl.de/de/seminars/seminar-calendar/seminar-details/08253

Presentationi in webinars su invito

1. Webinar: "Summer Seminars on Cybersecurity", "Cryptography for Blockchain Technology", 2021. www.diag.uniroma1.it/node/23436
2. Webinar: "Contact Tracing & Giant Data Collectors: A Journey from Utopia to Dystopia?", "The Gaze of the Gorgon, A Trojan Horse or An Offer We Could Not Refuse?", 2020. https://tracecorona.net/dec-2020-web-seminar-contact-tracing/
3. Launch event of a new research cluster "Cybersecurity, Design and Human Behaviour", "Blockchain Technology and Decentralized Contact Tracing: The Good, the Bad and the Ugly", 2020. https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/business-and-management/events/launch-event-of-a-new-research-
4. CS@GSSI/ICE-TCS webinar series, "There Is Something (Wrong) About Digital Contact Tracing", 2020. https://web.archive.org/web/20211203081742/https://sites.google.com/gssi.it/csgssi/seminars-and-events/

joint-ice-tcs-csgssi-virtual-seminar

Presentationi in conferenze/workshop/meeting in presenza

- Novembre 2023: Privacy-Enhanced Non-Fungible Tokens
  Ambito: Conferenza Secitc '23 *Luogo*: Bucarest, Romania

- Settembre 2023: Privacy-Enhanced Non-Fungible Tokens
  Ambito: Workshop Crossing 2023
  Luogo: Darmstadt, Germania

- Novembre 2022: Efficient NIZK Arguments with Straight-Line Simulation and Extraction
  Ambito: Conferenza CANS 2022
  Luogo: Abu Dhabi, EAU

- Febbraio 2020: Data Privacy in Blockchains: Theory and Practice
  Ambito: Workshop DLT '20
  Luogo: Ancona, Italia

- Giugno 2019: Tutorial Blockchain
  Ambito: Riunione Annuale GTTI '19
  Luogo: Pavia, Italia

- Febbraio 2019: On Deleting Data from a Blockchain
  Ambito: Workshop DLT '19
  Luogo: Pisa, Italia

- Febbraio 2019: Privacy-Preserving Blockchain
  Ambito: Workshop BLOCKCHAIN: la promessa di una tecnologia pervasiva, AFCEA
  Luogo: Roma, Italia

- Ottobre 2018: Delayed-Input Cryptographic Protocols.
  Ambito: Conferenza CANS '18
  Luogo: Napoli, Italia.

- Settembre 2018: Blockchain Technology Beyond Cryptocurrencies.
  Ambito: Conferenza RTSI '18
  Luogo: Palermo, Italia.

- Aprile 2018: Blockchain Technology: A Cryptographic Perspective.
  Ambito: Cryptography Seminar Series
  Luogo: Oxford, UK.

- Giugno 2017: Delayed-Input Cryptographic Protocols.
  Ambito: Conferenza CIE '17
  Luogo: Turku, Finlandia.

- Agosto 2017: Continuously Non-Malleable Codes in the Split-State Model from Minimal Assumptions.
  Ambito: Conferenza CRYPTO '17
  Luogo: Santa Barbara, California, USA

- Gennaio 2017: Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs
  Ambito: Conferenza ITASEC '17
  Luogo: Venezia, Italia

- Agosto 2015: Impossibility of Black-Box Simulation Against Leakage Attacks
  Ambito: Conferenza CRYPTO '15
  Luogo: Santa Barbara, California, USA

- Luglio 2015: New Techniques for OR Composition of Sigma Protocols and Their Applications
  Ambito: NTT
  Luogo: Mitaka - Giappone

- Marzo 2015: Constant-Round Concurrent Zero Knowledge from Indistinguishability Obfuscation
  Ambito: COST meeting on Secure Protocols
  Luogo: Varsavia, Poland

- Settembre 2014: On Selective-Opening Attacks Against Encryption Schemes
  Ambito: SCN '14
  Luogo: Amalfi - Italy

- Marzo 2013: On Defining Security of Proofs Systems via Witness Indistinguishability
  Ambito: NTT
  Luogo: Mitaka - Giappone

- Giugno 2012: The Round Complexity of (Concurrent, Resettable, Efficient) Zero Knowledge in the Bare Public-Key Model
  Ambito: Microsoft Research Colloquium '12
  Luogo: Redmond - USA

- Aprile 2012: Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions
  Ambito: Conferenza EUROCRYPT '12 (rump session)
  Luogo: Cambridge - UK

- Marzo 2012: Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions
  Ambito: Conferenza TCC '12 (rump session)
  Luogo: Taormina - Italia

- 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, 2009
  Luogo: La Jolla (CAL) - USA

- Novembre 2009: Revisiting RFID Security and Privacy
  Ambito: Distinguished Lecturer Seminar Series at UCI, 2009
  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, Track C
  Luogo: Reykjavik - Islanda

- Luglio 2008: Bounded Ciphertext-Policy Attribute-Based Encryption
  Ambito: Conferenza ICALP '08, Track C
  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

- Febbraio 2007: Concurrent Non-Malleable Witness Indistinguishability and Its Applications
  Ambito: Conferenza TCC '07 (rump session)
  Luogo: Amstedam, Paesi Bassi

- 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, Track C
  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, Track C
  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

Coordinamento e supervisione di attività di ricerca

1. Coordinatore di 5 "assegni per attività di ricerca" dell'Università di Salerno.
2. Coordinatore di 3 "borse di studio per attività di ricerca" dell'Università di Salerno.
3. Supervisione del dottorato di ricerca di Alessandra Scafuro (2009-2012), adesso associate professor, North Carolina State University (USA).
4. Supervisione del dottorato di ricerca di Luisa Siniscalchi (2014-2017), adesso assistant professor in tenure track, Danmarks Tekniske Universitet (DTU), Kongens Lyngby.
5. Supervisione del dottorato di ricerca di Vincenzo Botta (2018-22), adesso ricercatore post-doc presso la University of Warsaw.

6. Gennaro Avitabile (2019-23), adesso ricercatore post-doc presso IMDEA Software Institute, Madrid.

Attività editoriale e organizzazione di eventi

1. Editor della special issue "Advances in Security for Communication Networks" di "Journal of Computer Security", IOS press, 2013.
2. Co-editor dei Proceedings del Fifth Distributed Ledger Technology Workshop (DLT 2023), Bologna, Italy, CEUR Workshop Proceedings 3460. Altri co-editors: Stefano Bistarelli e Paolo Mori.
3. Co-editor dei proceedings relativi alla conferenza "The 8th Conference on Security and Cryptography for Networks (SCN 2012)" - (5 - 7 settembre 2012) - Amalfi, Italia, proceedings LNCS,Vol. 7485, Springer, Heidelberg, Germania, ISBN 978-3-642-32927-2. Altri co-editors: Roberto De Prisco.
4. Co-editor 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, Heidelberg, Germania, Agosto 2008, ISBN 978-3-540-85854-6. Altri co-editors: Rafail Ostrovsky, Roberto De Prisco.
5. Co-Organizer della "ECRYPT Autumn International School on Zero Knowledge: Foundations and Applications", Bertinoro, Italy, 2006.
   `http://tinyurl.com/zd72mmj`
6. Co-Organizzatore del Workshop on Cryptographic Protocols and Public-Key Cryptography, Bertinoro, Italy, 2009.
   `https://web.archive.org/web/20090608015335/http://wpk.dia.unisa.it/`
7. General Co-Chair di "The 6th Conference on Security and Cryptography for Networks (SCN 2008)" - Amalfi, Italia, Settembre 2008 - LNCS Springer-Verlag.
8. Organizzatore di 2 meeting internazionali relativi al Networks of Excellence ECRYPT e di un meeting internazionale realtivo al RIA-H2020 PRIViLEDGE.

Parte VIII – Riepilogo dei conseguimenti scientifici

Le pubblicazioni del sottoscritto apparse nei proceedings delle seguenti conferenze

1. *IEEE*: FOCS (2012, 2013)
2. *ACM*: CCS (2000), STOC (2014)
3. *IACR*: CRYPTO (2004, 2005, 2008, 2009, 2012 - 2 papers, 2015, 2016, 2017, 2018, 2019), EUROCRYPT (2012, 2013, 2015, 2016, 2017, 2020), ASIACRYPT (2004, 2013, 2018, 2019), TCC (2006, 2009, 2010, 2012 - 2 papers, 2013 - 2 papers, 2014 - 2 papers, 2016 - 2 papers, 2017 - 3 papers), PKC (2008, 2010, 2019, 2021).
4. *EATCS*: ICALP (2005 - 3 papers, 2006, 2008, 2012, 2014).
5. *Others*: ESORICS (2008, 2022), Financial Cryptography (2004, 2021), CT-RSA (2011), ACNS (2010, 2021)

lo pongono tra i ricercatori più proficui tra gli afferenti ad istituzioni italiane nel pubblicare nelle conferenze più prestigiose al mondo su temi di sicurezza informatica. Alla luce delle classi-

ficazioni di *csrankings.org*[1], considerando le aree "Cryptography" e "Computer security" (le due aree più aderenti alle linee di ricerca del sottoscritto) negli ultimi 10/20 anni Ivan Visconti è tra i migliori afferenti ad istituzioni italiane, con 17 pubblicazioni nel periodo 2004-2023 e 10 pubblicazioni nel periodo 2013-2023.

Anche considerando le statistiche delle prestigiose conferenze organizzate dall'*IACR*[2] il sottoscritto con 39 pubblicazioni nel periodo 2004-2023 e 24 pubblicazioni nel periodo 2013-2024 è tra i migliori afferenti ad istituzioni italiane.

Considerando il rating GII-GRIN-SCIE (GGS) [3], complessivamente

- 21 pubblicazioni del sottoscritto sono valutate A++ (il top) [CRYPTO 11+ EUROCRYPT 6 + STOC 1 + FOCS 2 + CCS 1]
- 20 sono valutate A+ [14 TCC + ASIACRYPT 4 + ESORICS 2]
- 41 sono classificate in classe 1 [A++ 21 + A+ 20]
- 13 sono valutate A [ICALP 7 + PKC 4 + FC 2]
- 15 sono classificate in classe 2 [A 13 + ACNS 2]

Considerando solo il periodo 2004-2023 abbiamo che

- 20 pubblicazioni sono valutate A++ (il top) [CRYPTO 11 + EUROCRYPT 6 + STOC 1 + FOCS 1]
- 20 sono valutate A+ [TCC14 + ASIACRYPT 4 + ESORICS 2]
- 40 sono classificate in classe 1 [A++ 20 + A+ 20]
- 13 sono valutate A [ICALP 7 + PKC 4 + FC 2]
- 15 sono classificate in classe 2 [A 13 + ACNS 2]

Considerando solo il periodo 2013-2023 abbiamo che

- 12 pubblicazioni sono valutate A++ (il top) [CRYPTO 5 + EUROCRYPT 5 + STOC 1 + FOCS 1]
- 13 sono valutate A+ [TCC 9 + ASIACRYPT 3 + ESORICS 1]
- 25 sono classificate in classe 1 [A++ 12 + A+ 13]
- 4 sono valutate A [ICALP 1 + PKC 2 + FC 1]
- 5 sono classificate in classe 2 [A 4 + ACNS 1]

Il sottoscritto è inoltre tra i pochi crittografi afferenti ad istituzioni italiane ad aver pubblicato a STOC e FOCS e ad essere stato membro del comitato di programma di almeno una delle due conferenze (per la precisione, FOCS 2018).

Il sottoscritto è stato 17 volte nei comitati di programma di conferenze IACR[4], di cui 12 volte nel periodo 2013-2023.

Il sottoscritto Ivan Visconti secondo Google Scholar e Scopus ha i seguenti parametri relativamente alle sue pubblicazioni senza restrizioni temporali.

1. Google Scholar Indice H: 30.
2. Google Scholar Numero totale citazioni: 2429.
3. Google Scholar i10-index: 66.

[1] `https://csrankings.org/#/fromyear/2004/toyear/2023/index?sec&crypt&it`

[2] `https://www.iacr.org/cryptodb/data/stats.php?crypto=on&eurocrypt=on&asiacrypt=on&ches=on&fse=on&pkc=on&tcc=on&tosc=on&tches=on&startyear=2004&endyear=2023`

[3] `https://scie.lcc.uma.es/`

[4] `https://www.iacr.org/cryptodb/data/author.php?authorkey=25`

4. Researcher Scopus ID: 8951609400.
5. Scopus Indice H: 20.
6. Scopus numero toale pubblicazioni: 97.
7. Scopus numero totale citazioni: 1127.
8. Anzianità accademica (anni trascorsi dalla laurea): 25.
9. H index normalizzato (H index complessivo diviso per l'anzianità accademica): 20/25=0.8.

Numero complessivo delle pubblicazioni a diffusione internazionale con revisione anonima tra pari (peer review) rilevate sulle banche dati internazionali riconosciute per l'abilitazione scientifica nazionale del settore scientifico-disciplinare oggetto della selezione: 92 (fonte Scopus).

Con esclusivo riferimento alle tipologie di prodotti valide per la partecipazione alle procedure di Abilitazione Scientifica Nazionale, in relazione all'arco temporale delle pubblicazioni selezionabili (2013-2023) si riporta quanto segue:

1. Numero complessivo di lavori su banche dati internazionali riconosciute per l'Abilitazione Scientifica Nazionale: 46 (fonte Scopus).
2. Indice di Hirsch: 13 (fonte Scopus).
3. Numero totale delle citazioni: 360 (fonte Scopus).
4. Numero medio di citazioni per pubblicazione: 360/46=7,83
5. Impact factor totale in relazione all'anno di pubblicazione: 11,92 (fonte Clarivate/Web of Science).
6. Numero pubblicazioni per le quali è disponibile l'impact factor in relazione all'anno di pubblicaione: 3 (fonte Clarivate/Web of Science).
7. Impact factor medio per pubblicazione: 11,92/3=3,97.

Part IX – Publicazioni selezionate

Per una elenco esteso delle pubblicazioni è possibile consultare il database Scopus database con author id 8951609400, google scholar `https://scholar.google.it/citations?user=QEairGEAAAAJ` e la DBLP computer science bibliography at `https://dblp.org/pid/81/5771.html`. Di seguito saranno elencate solo le pubblicazioni più significative.

Seguento uno standard diffuso nella comunità di ricerca del sottoscritto, in tutte le pubblicazioni gli autori sono elencati in order alfabetico, ed il contributo dei singoli autori è da considerarsi paritetico.

Seguono le 15 pubblicazioni selezionate nel periodo di riferimento 2013-2023 con il numero di citazioni indicato dal database Scopus.

1. Continuously Non-Malleable Codes in the Split-State Model from Minimal Assumptions.
   In proceedings of (**CRYPTO 2018**). Santa Barbara, USA, 2018.
   Lecture Notes in Computer Science, Vol. 10993, Pagg. 608-639, ISBN 978-3-319-96877-3, Springer, Heidelberg, Germania.
   Autori: Rafail Ostrovsky, Giuseppe Persiano, Daniele Venturi and Ivan Visconti.
   Citazioni: 18.

2. Four-Round Concurrent Non-Malleable Commitments from One-Way Functions.
   In proceedings of (**CRYPTO 2017**). Santa Barbara, USA, 2017.
   Lecture Notes in Computer Science, Vol. 10402, Pagg. 127-157, ISBN 978-3-319-63714-3, Springer, Heidelberg, Germania.
   Autori: Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi and Ivan Visconti.
   Citazioni: 22.

3. Concurrent Non-Malleable Commitments (and More) in 3 Rounds.
   In proceedings of the 35th Annual IACR Crypto Conference (**CRYPTO 2016**). Santa Barbara, USA.
   Lecture Notes in Computer Science, Vol. 9816, Pagg. 270-299, ISBN 978-3-662-53014-6, Springer, Heidelberg, Germania, 2016.
   Autori: Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, Ivan Visconti.
   Citazioni: 25.

4. How to Extract Useful Randomness from Unreliable Sources.
   In proceedings of (**EUROCRYPT 2020**). Zagreb, Croatia, 2020.
   Lecture Notes in Computer Science, Vol. 12105, Pagg. 343-372, ISBN 978-3-030-45720-4, Springer, Heidelberg, Germania.
   Autori: Divesh Aggarwal, Maciej Obremski, João Ribeiro, Luisa Siniscalchi e Ivan Visconti.
   Citazioni: 5.

5. Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs.
   In proceedings of (**EUROCRYPT 2017**). Parigi, Francia, 2017.
   Lecture Notes in Computer Science, Vol. 10210, Pagg. 382-411, ISBN 978-3-319-56619-1, Springer, Heidelberg, Germania.
   Autori: Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, Ivan Visconti.
   Citazioni: 15.

6. Online/Offline OR Composition of Sigma Protocols.
   In proceedings of (**EUROCRYPT 2016**). Vienna, Austria, 2016.
   Lecture Notes in Computer Science, Vol. 9666, Pagg. 63-92, ISBN 978-3-662-49895-8, Springer, Heidelberg, Germania.
   Autori: Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, Ivan Visconti.
   Citazioni: 20.

7. Executable Proofs, Input-Size Hiding Secure Computation and a New Ideal World.
   In proceedings of the 34th IACR Conference (**EUROCRYPT 2015**). April 26-30, 2015, Sofia, Bulgaria.
   Lecture Notes in Computer Science, Vol. 9057, Pagg. 532-560, ISBN 978-3-662-46802-9, Springer, Heidelberg, Germania, 2015.
   Autori: Melissa Chase, Rafail Ostrovsky, Ivan Visconti.
   Citazioni: 6.

8. Black-Box Non-Black-Box Zero Knowledge.
   In proceedings of (**STOC 2014**). New York, USA.
   Pagg. 515-524, ACM Press, ISBN 978-1-4503-2710-7.
   Autori: Vipul Goyal, Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti.
   Citazioni: 24.

9. Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions.
   In proceedings of (**EUROCRYPT 2013**). Athens, Greece.
   Lecture Notes in Computer Science, Vol. 7781, Pagg. 702-718, ISBN 978-3-642-38347-2, Springer, Heidelberg, Germany, to appear.
   Autori: Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti, Akshay Wadia.
   Citazioni: 46.

10. Simultaneous Resettability from One-Way Functions.
    In proceedings of (**FOCS 2013**). Berkeley, USA.
    Pagg. 60-69,IEEE, ISBN 978-0-7695-5135-7, 2013.
    Autori: Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Ivan Visconti.
    Citazioni: 16.

11. 4-Round Resettably-Sound Zero Knowledge.
    In proceedings of (**TCC 2014**). San Diego, USA.
    Lecture Notes in Computer Science, Vol. 8349, Pagg. 192-216, ISBN 978-3-642-54241-1, Springer, Heidelberg, Germania.
    Autori: Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, Ivan Visconti.
    Citazioni: 18.

12. Improved OR Composition of Sigma-protocols.
    In proceedings of (**TCC 2016**). Tel Aviv, Israel, 2016.
    Lecture Notes in Computer Science, Vol. 9563, Pagg. 112-141, ISBN 978-3-662-49098-3, Springer, Heidelberg, Germania.
    Autori: Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, Ivan Visconti.
    Citazioni: 26.

13. A Transform for NIZK Almost as Efficient and General as the Fiat-Shamir Transform Without Programmable Random Oracles.
    In proceedings of (**TCC 2016**). Tel Aviv, Israel.
    Lecture Notes in Computer Science, Vol. 9563, Pagg. 83-111, ISBN 978-3-662-49098-3, Springer, Heidelberg, Germania, 2016.
    Autori: Michele Ciampi, Giuseppe Persiano, Luisa Siniscalchi, Ivan Visconti.
    Citazioni: 23.

14. Delayed-Input Non-Malleable Zero Knowledge and Multi-Party Coin Tossing in Four Rounds.
    In proceedings of (**TCC 2017**). Baltimore, USA, 2017.
    Lecture Notes in Computer Science, Vol. 10677, Pagg. 711-742, ISBN 978-3-319-70499-9, Springer, Heidelberg, Germania.
    Autori: Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi and Ivan Visconti.
    Citazioni: 16.

15. Round-Optimal Secure Two-Party Computation from Trapdoor Permutations.
    In proceedings of (**TCC 2017**). Baltimore, USA, 2017.
    Lecture Notes in Computer Science, Vol. 10677, Pagg. 678-710, ISBN 978-3-319-70499-9, Springer, Heidelberg, Germania.
    Autori: Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi and Ivan Visconti.
    Citazioni: 14.

Per convenienza, di seguito c'è una lista delle principali pubblicazioni, sull'intera carriera del sottoscritto.

- 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.

- 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 e Ivan Visconti.

- 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.

- 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.

- 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.

- Concurrent Zero Knowledge in the Public-Key Model.
  In proceedings of the 32nd International Colloquium on Automata, Languages and Programming (**ICALP 05**, Track C). 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.

- Hybrid Trapdoor Commitments and Their Applications.
  In proceedings of the 32nd International Colloquium on Automata, Languages and Programming (**ICALP 05**, Track C). 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.

- Single-Prover Concurrent Zero Knowledge in Almost Constant Rounds.
  In proceedings of the 32nd International Colloquium on Automata, Languages and Programming (**ICALP 05**, Track C). 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.

- 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.

- 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.

- Efficient Zero Knowledge on the Internet.
  In proceedings of the 33rd International Colloquium on Automata, Languages and Programming (**ICALP 06**, Track C). 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.

- 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.

- 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.

- 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**, Track C). 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.

- 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.

- 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, ISBN 978-3-540-88312-8, Springer-Verlag, Heidelberg, Germania, Ottobre 2008.
  Autori: Carlo Blundo, Giuseppe Persiano, Ahmad-Reza Sadeghi, Ivan Visconti.

- 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, Vol. 5444, Pagg. 91-108, ISBN 978-3-642-00456-8, Heidelberg, Germania.
  Autori: Rafail Ostrovsky, Giuseppe Persiano, Ivan Visconti.

- 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, Vol. 5677, Pagg. 524-540, ISBN 978-3-642-03355-1, Springer-Verlag, Heidelberg, Germania, Agosto 2009.
  Autori: Joël Alwen, Jonathan Katz, Yehuda Lindell,Giuseppe Persiano, Abhi Shelat e Ivan Visconti.

- 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, ISSN 0302-9743.
  Autori: Frederik Armknecht, Ahmad-Reza Sadeghi, Alessandra Scafuro, Ivan Visconti, Christian Wachsmann.

- 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, Vol. 5444, Pagg. 91-108, ISBN 978-3-642-00456-8, Springer, Heidelberg, Germania.
  Autori: Rafail Ostrovsky, Omkant Pandey, Ivan Visconti.

- 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, Vol. 6123, Pagg. 493-510, ISBN 978-3-642-13707-5, Springer, Heidelberg, Germania, 2010.
  Autori: Frederik Armknecht, Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann.

- 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, Vol. 6056, Pagg. 193-208, ISBN 978-3-642-13012-0, Springer, Heidelberg, Germania, 2010.
  Autori: Zhenfu Cao, Ivan Visconti, Zongyang Zhang.

- 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, Vol. 6558, Pagg. 1-16, ISBN 978-3-642-19073-5, Springer, Heidelberg, Germania, 2011.
  Autori: Marc Fischlin, Benny Pinkas, Ahmad-Reza Sadeghi, Thomas Schneider, Ivan Visconti.

- Statistical Resettable Zero Knowledge.
  In proceedings of the 9th Theory of Cryptography Conference (**TCC 2012**). March 19-21,

Taormina, Italy.
Lecture Notes in Computer Science, Vol. 7194, Pagg. 494-512, ISBN 978-3-642-29010-7, Springer, Heidelberg, Germania, 2012.
Autori: Sanjam Garg, Rafail Ostrovsky, Ivan Visconti, Akshay Wadia.

- Simultaneously Resettable Arguments of Knowledge.
  In proceedings of the 9th Theory of Cryptography Conference (**TCC 2012**). March 19-21, Taormina, Italy.
  Lecture Notes in Computer Science, Vol. 7194, Pagg. 530-547, ISBN 978-3-642-29010-7, Springer, Heidelberg, Germania, 2012.
  Autori: Chongwon Cho, Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti.

- On Round-Optimal Zero Knowledge in the Bare Public-Key Model.
  In proceedings of (**EUROCRYPT 2012**). April 18-21, Cambridge, UK.
  Lecture Notes in Computer Science, Vol. 7237, Pagg. 153-171, ISBN 978-3-642-29010-7, Springer, Heidelberg, Germania, 2012.
  Autori: Alessandra Scafuro, Ivan Visconti.

- Nearly Simultaneously Resettable Black-Box Zero Knowledge.
  In proceedings of the 39th International Colloquium on Automata, Languages and Programming (**ICALP 12**, Track A). July 9-13, 2012, Warwick - UK.
  Lecture Notes in Computer Science, Vol. 7391, Pagg. 88-99, ISBN 978-3-642-31593-0, Springer, Heidelberg, Germania, 2012.
  Autori: Joshua Baron, Rafail Ostrovsky, Ivan Visconti.

- Secure Database Commitments and Universal Arguments of Quasi Knowledge.
  In proceedings of the 32nd Annual IACR Crypto Conference (**CRYPTO 2012**). August 19-23, 2012, Santa Barbara, USA.
  Lecture Notes in Computer Science, Vol. 7417, Pagg. 236-254, ISBN 978-3-642-32008-8, Springer, Heidelberg, Germania, 2012.
  Autori: Melissa Chase, Ivan Visconti.

- Impossibility Results for Static Input Secure Computation.
  In proceedings of the 32nd Annual IACR Crypto Conference (**CRYPTO 2012**). August 19-23, 2012, Santa Barbara, USA.
  Lecture Notes in Computer Science, Vol.7417, Pagg. 424-442, ISBN 978-3-642-32008-8, Springer, Heidelberg, Germania, 2012.
  Autori: Sanjam Garg, Abishek Kumarasubramanian, Rafail Ostrovsky, Ivan Visconti.

- Constructing Non-Malleable Commitments: A Black-Box Approach.
  In proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (**FOCS 2012**). October 20-23, 2012, New Brunswick, New Jersey, USA.
  IEEE, Pagg. 51-60, ISBN 978-1-4673-4383-1, 2012.
  Autori: Vipul Goyal and Chen-Kuei Lee and Rafail Ostrovsky, Ivan Visconti.

- Revisiting Lower and Upper Bounds for Selective Decommitments.
  In proceedings of the 10th Theory of Cryptography Conference (**TCC 2013**). March 3-6, Tokyo, Japan.
  Lecture Notes in Computer Science, Vol. 7785, Pagg. 559-578, ISBN 978-3-642-36593-5, Springer, Heidelberg, Germania, 2013.
  Autori: Rafail Ostrovsky, Vanishree Rao, Alessandra Scafuro, Ivan Visconti.

- Concurrent Zero Knowledge in the Bounded Player Model.
  In proceedings of the 10th Theory of Cryptography Conference (**TCC 2013**). March 3-6, Tokyo, Japan.
  Lecture Notes in Computer Science, Vol. 7785, Pagg. 60-79, ISBN 978-3-642-36593-5, Springer, Heidelberg, Germania, 2013.
  Autori: Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, Ivan Visconti.

- Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions.
  In proceedings of (**EUROCRYPT 2013**). Athens, Greece.
  Lecture Notes in Computer Science, Vol. 7781, Pagg. 702-718, ISBN 978-3-642-38347-2, Springer, Heidelberg, Germany, to appear.
  Autori: Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti, Akshay Wadia.

- Constant-Round Concurrent Zero Knowledge in the Bounded Player Model.
  In proceedings of the 19th Annual International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT 2013**). December 1-5, Bangalore, India.
  Lecture Notes in Computer Science, Vol. 8268, Pagg. 21-40, ISBN 978-3-642-42032-0, Springer, Heidelberg, Germania, 2013.
  Autori: Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, Ivan Visconti.

- Simultaneous Resettability from One-Way Functions.
  In proceedings of (**FOCS 2013**). Berkeley, USA.
  Pagg. 60-69,IEEE, ISBN 978-0-7695-5135-7, 2013.
  Autori: Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Ivan Visconti.

- Statistical Concurrent Non-malleable Zero Knowledge.
  In proceedings of (**TCC 2014**). San Diego, USA.
  Lecture Notes in Computer Science, Vol. 8349, Pagg. 167-191, ISBN 978-3-642-54241-1, Springer, Heidelberg, Germania.
  Autori: Claudio Orlandi, Rafail Ostrovsky, Vanishree Rao, Amit Sahai, Ivan Visconti.

- 4-Round Resettably-Sound Zero Knowledge.
  In proceedings of (**TCC 2014**). San Diego, USA.
  Lecture Notes in Computer Science, Vol. 8349, Pagg. 192-216, ISBN 978-3-642-54241-1, Springer, Heidelberg, Germania.

Autori: Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, Ivan Visconti.

- Black-Box Non-Black-Box Zero Knowledge.
  In proceedings of (**STOC 2014**). New York, USA.
  Pagg. 515-524, ACM Press, ISBN 978-1-4503-2710-7.
  Autori: Vipul Goyal, Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti.

- On Input Indistinguishable Proof Systems.
  In proceedings of the 41th International Colloquium on Automata, Languages and Programming (**ICALP 14**, Track A). July 8-11, 2014, Copenhagen - Denmark.
  Lecture Notes in Computer Science, Vol. 8572, Pagg. 805-906, ISBN 978-3-662-43947-0, Springer, Heidelberg, Germania, 2014.
  Autori: Rafail Ostrovsky, Giuseppe Persiano, Ivan Visconti.

- Executable Proofs, Input-Size Hiding Secure Computation and a New Ideal World.
  In proceedings of the 34th IACR Conference (**EUROCRYPT 2015**). April 26-30, 2015, Sofia, Bulgaria.
  Lecture Notes in Computer Science, Vol. 9057, Pagg. 532-560, ISBN 978-3-662-46802-9, Springer, Heidelberg, Germania, 2015.
  Autori: Melissa Chase, Rafail Ostrovsky, Ivan Visconti.

- Impossibility of Black-Box Simulation Against Leakage Attacks.
  In proceedings of the 35th Annual IACR Crypto Conference (**CRYPTO 2015**), Santa Barbara, USA.
  Lecture Notes in Computer Science, Vol. 9216 Pagg. 130-149, ISBN 978-3-662-47999-5, Springer, Heidelberg, Germania, 2015.
  Autori: Rafail Ostrovsky, Giuseppe Persiano, Ivan Visconti.

- A Transform for NIZK Almost as Efficient and General as the Fiat-Shamir Transform Without Programmable Random Oracles.
  In proceedings of (**TCC 2016**). Tel Aviv, Israel.
  Lecture Notes in Computer Science, Vol. 9563, Pagg. 83-111, ISBN 978-3-662-49098-3, Springer, Heidelberg, Germania, 2016.
  Autori: Michele Ciampi, Giuseppe Persiano, Luisa Siniscalchi, Ivan Visconti.

- Improved OR Composition of Sigma-protocols.
  In proceedings of (**TCC 2016**). Tel Aviv, Israel, 2016.
  Lecture Notes in Computer Science, Vol. 9563, Pagg. 112-141, ISBN 978-3-662-49098-3, Springer, Heidelberg, Germania.
  Autori: Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, Ivan Visconti.

- Online/Offline OR Composition of Sigma Protocols.
  In proceedings of (**EUROCRYPT 2016**). Vienna, Austria, 2016.

Lecture Notes in Computer Science, Vol. 9666, Pagg. 63-92, ISBN 978-3-662-49895-8, Springer, Heidelberg, Germania.
Autori: Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, Ivan Visconti.

- Concurrent Non-Malleable Commitments (and More) in 3 Rounds.
  In proceedings of the 35th Annual IACR Crypto Conference (**CRYPTO 2016**). Santa Barbara, USA.
  Lecture Notes in Computer Science, Vol. 9816, Pagg. 270-299, ISBN 978-3-662-53014-6, Springer, Heidelberg, Germania, 2016.
  Autori: Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, Ivan Visconti.

- Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs.
  In proceedings of (**EUROCRYPT 2017**). Parigi, Francia, 2017.
  Lecture Notes in Computer Science, Vol. 10210, Pagg. 382-411, ISBN 978-3-319-56619-1, Springer, Heidelberg, Germania.
  Autori: Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, Ivan Visconti.

- Delayed-Input Non-Malleable Zero Knowledge and Multi-Party Coin Tossing in Four Rounds.
  In proceedings of (**TCC 2017**). Baltimore, USA, 2017.
  Lecture Notes in Computer Science, Vol. 10677, Pagg. 711-742, ISBN 978-3-319-70499-9, Springer, Heidelberg, Germania.
  Autori: Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi and Ivan Visconti.

- Round-Optimal Secure Two-Party Computation from Trapdoor Permutations.
  In proceedings of (**TCC 2017**). Baltimore, USA, 2017.
  Lecture Notes in Computer Science, Vol. 10677, Pagg. 678-710, ISBN 978-3-319-70499-9, Springer, Heidelberg, Germania.
  Autori: Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi and Ivan Visconti.

- Resettably-Sound Resettable Zero Knowledge in Constant Rounds.
  In proceedings of (**TCC 2017**). Baltimore, USA, 2017.
  Lecture Notes in Computer Science, Vol. 10677, Pagg. 111-138, ISBN 978-3-319-70499-9, Springer, Heidelberg, Germania.
  Autori: Wutichai Chongchitmate, Rafail Ostrovsky e Ivan Visconti.

- Four-Round Concurrent Non-Malleable Commitments from One-Way Functions.
  In proceedings of (**CRYPTO 2017**). Santa Barbara, USA, 2017.
  Lecture Notes in Computer Science, Vol. 10402, Pagg. 127-157, ISBN 978-3-319-63714-3, Springer, Heidelberg, Germania.
  Autori: Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi and Ivan Visconti.

- Continuously Non-Malleable Codes in the Split-State Model from Minimal Assumptions.
  In proceedings of (**CRYPTO 2018**). Santa Barbara, USA, 2018.
  Lecture Notes in Computer Science, Vol. 10993, Pagg. 608-639, ISBN 978-3-319-96877-3,

Springer, Heidelberg, Germania.
Autori: Rafail Ostrovsky, Giuseppe Persiano, Daniele Venturi and Ivan Visconti.

- Non-interactive Secure Computation from One-Way Functions.
  In proceedings of (**ASIACRYPT 2018**). Brisbane, Australia, 2018.
  Lecture Notes in Computer Science, Vol. 11274, Pagg. 118-138, ISBN 978-3-030-03331-6, Springer, Heidelberg, Germania.
  Autori: Saikrishna Badrinarayanan, Abhishek Jain, Rafail Ostrovsky and Ivan Visconti.

- Publicly Verifiable Proofs from Blockchains.
  In proceedings of (**PKC 2019**). Pechino, Cina, 2019.
  Lecture Notes in Computer Science, Vol. 11442, Pagg. 374-401, ISBN 978-3-030-17252-7, Springer, Heidelberg, Germania.
  Autori: Alessandra Scafuro, Luisa Siniscalchi and Ivan Visconti.

- Universally Composable Secure Computation with Corrupted Tokens.
  In proceedings of (**CRYPTO 20198**). Santa Barbara, USA, 2018.
  Lecture Notes in Computer Science, Vol. 11694, Pagg. 432-461, ISBN 978-3-030-26953-1, Springer, Heidelberg, Germania.
  Autori: Nishanth Chandran, Wutichai Chongchitmate, Rafail Ostrovsky and Ivan Visconti.

- UC-Secure Multiparty Computation from One-Way Functions Using Stateless.
  In proceedings of (**ASIACRYPT 2019**). Kobe, Japan, 2019.
  Lecture Notes in Computer Science, Vol. 11922, Pagg. 577-605, ISBN 978-3-030-34620-1, Springer, Heidelberg, Germania.
  Autori: Saikrishna Badrinarayanan, Abhishek Jain, Rafail Ostrovsky and Ivan Visconti.

- How to Extract Useful Randomness from Unreliable Sources.
  In proceedings of (**EUROCRYPT 2020**). Zagreb, Croatia, 2020.
  Lecture Notes in Computer Science, Vol. 12105, Pagg. 343-372, ISBN 978-3-030-45720-4, Springer, Heidelberg, Germania.
  Autori: Divesh Aggarwal, Maciej Obremski, João Ribeiro, Luisa Siniscalchi e Ivan Visconti.

- Publicly Verifiable Zero Knowledge from (Collapsing) Blockchains.
  In proceedings of (**PKC 2021**). 2021.
  Lecture Notes in Computer Science, Vol. 12711, Pagg. 469-498, ISBN 978-3-030-75247-7, Springer, Heidelberg, Germania.
  Autori: Alessandra Scafuro, Luisa Siniscalchi and Ivan Visconti.

- Terrorist Attacks for Fake Exposure Notifications in Contact Tracing Systems.
  In proceedings of the 8th International Conference on Applied Cryptography and Network Security (**ACNS 2021**), 2021.
  Lecture Notes in Computer Science, Vol. 12726, Pagg. 220-247, ISBN 978-3-030-78371-6, Springer, Heidelberg, Germania, 2021.
  Autori: Gennaro Avitabile, Daniele Friolo e Ivan Visconti.

- Shielded Computations in Smart Contracts Overcoming Forks.
  In proceedings of (**FC 2021**). 2021.
  Lecture Notes in Computer Science, Vol. 12674, Pagg. 73-92, ISBN 978-3-662-64321-1, Springer, Heidelberg, Germania.
  Autori: Vincenzo Botta, Daniele Friolo, Daniele Venturi e Ivan Visconti.

- Efficient Proofs of Knowledge for Threshold Relations.
  In proceedings of (**ESORICS 2022**). 2022.
  Lecture Notes in Computer Science, Vol. 12674, Pagg. 42-62, ISBN 978-3-031-17142-0, Springer, Heidelberg, Germania.
  Autori: Gennaro Avitabile, Vincenzo Botta, Daniele Friolo e Ivan Visconti.

- Efficient NIZK Arguments with Straight-Line Simulation and Extraction.
  In proceedings of (**CANS 2022**). 2022.
  Lecture Notes in Computer Science, Vol. 13641, Pagg. 2-22, ISBN 978-3-031-20973-4, Springer, Heidelberg, Germania.
  Autori: Miche Ciampi e Ivan Visconti.

- Towards Data Redaction in Bitcoin.
  IEEE Trans. Netw. Serv. Manag., Vol. 19, Num. 4, Pagg. 3872-3883, ISSN:1932-4537.
  Autori: Vincenzo Botta, Vincenzo Iovino, Ivan Visconti.

- Towards Data Redaction in Bitcoin.
  In proceedings of (**CANS 2022**). 2022.
  Lecture Notes in Computer Science, Vol. 13641, Pagg. 2-22, ISBN 978-3-031-20973-4, Springer, Heidelberg, Germania.
  Autori: Miche Ciampi e Ivan Visconti.

- Digital Contact Tracing Solutions: Promises, Pitfalls and Challenges.
  IEEE Transactions on Emerging Topics in Computing, 2022.
  DOI: `https://doi.org/10.1109/TETC.2022.3216473`
  Autori: Thien Duc Nguyen, Markus Miettinen, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, Ivan Visconti.

- Doubly adaptive zero-knowledge proofs.
  Theoretical Computer Science, Elsevier (**TCS**), vol. 968, n. 114014, 2023, ISSN: 0304-3975.
  Autori: Vincenzo Botta, Ivan Visconti.

- Privacy and Integrity Threats in Contact Tracing Systems and Their Mitigations.
  IEEE Internet Comput., vol. 27, pp. 13-19, 2023, ISSN: 1089-7801.
  Autori: Gennaro Avitabile, Vincenzo Botta, Vincenzo Iovino, Ivan Visconti.

Salerno, 13 Dicembre 2023 Ivan Visconti