ALLEGATO A

UNIVERSITÀ DEGLI STUDI DI MILANO
Procedura di valutazione per la chiamata a professore di II fascia da ricoprire ai sensi dell'art. 24, comma 6, della Legge n. 240/2010 per il settore concorsuale 01/B1 INFORMATICA, (settore scientifico-disciplinare INF01 - INFORMATICA) presso il Dipartimento di Informatica "Giovanni degli Antoni", Codice concorso 4413

Andrea Visconti
CURRICULUM VITAE

INFORMAZIONI PERSONALI

Cognome	Visconti
Nome	Andrea
Data di nascita	05/06/1975

SOMMARIO

1 ESPERIENZE PROFESSIONALI E FORMAZIONE

1.1 Posizione attuale

Da Sett 2006 a oggi	Ricercatore (INF/01) a tempo indeterminato Università degli Studi di Milano, Dipartimento di Informatica "Giovanni Degli Antoni".

1.2 Esperienze pregresse

Da Sett 2015 a Sett 2018	Professore a Contratto Università degli Studi di Trento, Dipartimento di Matematica.
Feb 2012	Guest Researcher National Institute of Standards and Technology (NIST), Dipartimento del Commercio, Governo degli Stati Uniti.
Da Sett 2005 a Sett 2006	Professore a Contratto Università degli Studi dell'Insubria, Dipartimento di Informatica.
Da Nov 2002 ad Ago 2006	Assegnista di Ricerca Università degli Studi di Milano, Dipartimento di Informatica.

1.3 Abilitazioni

Da Gen 2020 a Gen 2029	Abilitazione Scientifica Nazionale 2018-2020, Settore concorsuale 09/H1, Sistemi di elaborazione delle informazioni.
Da Gen 2020 a Gen 2029	Abilitazione Scientifica Nazionale 2018-2020, Settore concorsuale 01/B1, Informatica.

1.4 Formazione

2005	Dottorato in Informatica, Università degli Studi di Milano. Titolo tesi di Dottorato: "Intrusion Detection via Artificial Immune Systems".
2001	Laurea in Informatica (110/110 e Lode) Università degli Studi di Milano. Titolo tesi di Laurea: "Crittoanalisi di RSA: proposta di una metodologia di attacco basata su alcune regolarità dello spazio delle chiavi".

2 ATTIVITÀ DI RICERCA

2.1 Inquadramento generale

L'attività di ricerca svolta dal 2004 ad oggi ha preso spunto dal mio interesse per lo studio di due grandi aree:

A. Modelli per la protezione dell'informazione nel contesto della trasmissione dati nello spazio e nel tempo
    - High-Speed Cryptography (HSC);
    - Key Derivation Functions (KDF);
    - Tecnologia blockchain;
    - Lightweight Cryptography e sicurezza in ambito IoT;
    - Codici di rilevazione e correzione degli errori;
    - Transazioni commerciali e crittografia.
B. Modelli per il riconoscimento delle intrusioni
    - Sistemi immunitari artificiali.

2.1.1 Modelli per la protezione dell'informazione nello spazio e nel tempo

High-Speed Cryptography

La trasmissione dei dati nello spazio richiede l'implementazione di primitive crittografiche ottimizzate e sicure, sia in hardware che in software. Non è difficile immaginare i contesti applicativi se si pensa a server di rete sovraccarichi o a dispositivi IoT con stringenti vincoli di risorse. Poiché molte operazioni crittografiche sfruttano la moltiplicazione polinomiale, l'aritmetica dei polinomi su campi finiti svolge un ruolo chiave nelle implementazioni software pre- e post-quantum. In questo contesto, abbiamo proposto un'ottimizzazione ricorsiva dell'algoritmo di Karatsuba per ridurre il numero di operazioni binarie necessarie a moltiplicare polinomi di grado n e l'uso di estensioni algebriche di GF(2) combinate con l'interpolazione di Lagrange per migliorare la complessità asintotica del prodotto polinomiale. Una seconda problematica affrontata in questo contesto è quella della minimizzazione di circuiti booleani di una determinata funzione crittografica. Rappresentazioni minimizzate, infatti, consentono sia l'implementazione di software crittografici veloci, sia implementazioni hardware che necessitano di un minor quantitativo di risorse. In questo contesto abbiamo proposto un'euristica greedy che lavora ottimamente quando la rappresentazione algebrica degli algoritmi crittografici mette in evidenza sistemi lineari densi. Le attività di ricerca svolte in quest'area, iniziate nel 2011 e ancora in fase di svolgimento, sono sfociate nel febbraio 2012 in una attività di visiting presso l'Information Technology Lab del NIST, Dipartimento del Commercio, Governo degli Stati Uniti e in una successiva collaborazione con i ricercatori dello stesso. Le attività precedentemente descritte hanno portato alla pubblicazione dei seguenti lavori [2,8,18,23].

Key Derivation Functions

La trasmissione di dati nel tempo (codici crittografici per la memorizzazione di informazioni a lungo termine) deve affrontare due problematiche rilevanti: l'esposizione verso il mondo esterno di una quantità di crittotesto pressoché illimitata e la possibilità di analizzare/attaccare off-line questo crittotesto per un periodo di tempo illimitato. La sicurezza dell'intero sistema crittografico si basa sulla conoscenza di uno o più segreti, solitamente password o passphrase, spesso aventi bassa entropia e definiti da utenti più o meno esperti. Per evitare di utilizzare direttamente tali segreti come chiavi crittografiche, solitamente si adottano le password-based Key Derivation Functions (KDF), un insieme di funzioni crittografiche che prendendo in input i segreti forniti dall'utente, generando un flusso di bit pseudocasuale di lunghezza arbitraria. Questo flusso ha sufficiente entropia per poter essere utilizzato come chiave nelle applicazioni del mondo reale. La key derivation function più utilizzata è PBKDF2. Introdotta nel 1999 dagli RSA Labs, è stata implementata da Goolge in Android, nei protocolli di sicurezza WPA/WPA2 sviluppati in ambito

Wi-Fi, in FileVault Mac OS X, negli archivi con formato di compressione RAR, in Linux con GRUB2 e LUKS, nei servizi online per la protezione di chiavi private di possessori di crittovaluta, etc. La forza delle KDF è data dall'introduzione di operazioni "CPU- e/o memory-intensive" non particolarmente onerose per l'utente onesto ma molto dispendiose per gli attaccanti. Queste operazioni consentono di ridurre drasticamente le probabilità di successo degli attacchi noti in letteratura. In questo contesto ci siamo occupati di studiare, analizzare e testare le primitive crittografiche implementate nelle KDF. L'attività di ricerca svolta nel periodo 2014-2019 ha evidenziato una serie di problematiche sia teoriche sia implementative delle primitive crittografiche adottate di default da PBKDF2 [1,5,17,20,21]. In tali lavori abbiamo sperimentalmente dimostrato come gli inconsapevoli utenti giocano un ruolo fondamentale nel ridurre la sicurezza di un sistema, per esempio scegliendo funzioni crittografiche più o meno performanti, adottando particolari opzioni di risparmio energetico o installando determinate librerie. Questa attività ha consentito l'individuazione e la correzione di bugs in librerie note e largamente utilizzate e se ne ha riscontro attraverso i seguenti link: gnupg.org e kernel.org.

Tecnologia blockchain

Una seconda problematica affrontata, sempre relativa alla protezione dei dati nel tempo, è quella della tutela del diritto d'autore di giovani artisti attraverso l'uso di tecniche crittografiche implementate in sistemi basati su blockchain. Tale attività, finanziata attraverso la vincita di un bando Cariplo 2017-2019, e svolta in collaborazione con l'Accademia di Brera e il Dipartimento di Beni Culturali e Ambientali di UniMi, era finalizzata a promuovere un impatto culturale sul territorio e sul tessuto sociale. Gli obiettivi del progetto, oltre alla protezione del diritto d'autore, sono stati la sperimentazione di un modello inedito di certificazione estetica (Dipartimento di Beni Culturali e Ambientali) e la valorizzazione di nuovi talenti artistici (Accademia di Brera). Questa attività di ricerca applicata è risultata anche vincitrice del premio "Idee Vincenti", iniziativa ideata e sostenuta da Lottomatica in collaborazione con il Politecnico di Milano (Polihub), il cui obiettivo era quello di premiare nuove idee basate su tecnologie avanzate per sostenere lo sviluppo innovativo del patrimonio artistico e culturale italiano. L'idea progettuale, dopo aver ricevuto l'approvazione dei dipartimenti coinvolti (luglio-ottobre 2018) e l'approvazione dal CDA di UniMi, è sfociata nella creazione dello spin-off AuthclicK srl nel febbraio 2019, spin-off di cui sono co-founder e membro del CDA.

Lightweight Cryptography e sicurezza in ambito IoT

In ambitio IoT, dal 2017 a oggi, abbiamo affrontato diverse problematiche legate (a) agli aspetti di sicurezza delle applicazioni in esecuzione, (b) alle performance di algoritmi crittografici e protocolli di comunicazione e (c) al riconoscimento di specifiche attività sulla base dei dati raccolti da sensori. Nel primo caso ci siamo occupati degli utenti che desiderano accedere ai propri account e mantenere tutti i dati sincronizzati, condividendo informazioni personali tramite Mobile Cloud Computing. Spesso accade che i dispositivi vengono sbloccati dagli utenti per garantire massimi privilegi alle applicazioni in esecuzione. In questo contesto, abbiamo sperimentalmente dimostrato che un utente malintenzionato potrebbe intercettare e raccogliere dati riservati di applicazioni in esecuzione [9,19]. Nel secondo caso ci siamo occupati di migliorare la sicurezza e le performance di algoritmi crittografici di tipo substitution–permutation network in un contesto "white-box", contesto nel quale gli avversari sono in grado accedere fisicamente all'algoritmo utilizzato e alla piattaforma sulla quale si eseguono gli esperimenti [6,16]. Nel terzo e ultimo caso, abbiamo proposto un approccio per il monitoraggio e l'individuazione delle attività degli individui con l'obiettivo di rilevare i cambiamenti nel modello comportamentale e nello stile di vita [4,7].

Codici di rilevazione e correzione degli errori

Per quel che riguarda i codici correttori, l'attività in questione ci ha visti coinvolti su diversi fronti. Nel biennio 2018-2019, ci siamo occupati dei supporti digitali per l'archiviazione dei dati largamente utilizzati negli ultimi 20 anni per la memorizzazione e la conservazione del patrimonio artistico e culturale del nostro paese. Questi supporti hanno una aspettativa di vita che è inadeguata rispetto alle effettive esigenze delle istituzioni. Pertanto, grazie a una collaborazione con il personale del Dipartimento di Chimica Industriale "Toso Montanari" dell'Università degli

Studi di Bologna, abbiamo affrontato la problematica di alleviare gli effetti dell'invecchiamento sui dischi ottici attraverso l'uso di un codice adattivo Reed-Solomon (A-RS). Tale codice consente di ridurre la capacità di correzione degli errori in aree considerate sicure e lo aumenta in aree considerate critiche [10].

Nel 2012 abbiamo affrontato il problema della pirateria nei sistemi di distribuzione di contenuti digitali. In questo contesto ci siamo occupati dei traitor tracing schemes, cioè schemi di rilevazione di utenti disonesti. L'obiettivo di questi schemi è consentire al tracciante di identificare almeno un utente disonesto. In questo contesto, abbiamo presentato una soluzione che migliorava lo stato dell'arte consentendo di eliminare le restrizioni sulla tipologia di utenti disonesti riconosciuti dallo schema. In particolare, abbiamo modificato un tipico schema di tracciamento dimostrando che un decoder pirata non è in grado di riconoscere pacchetti di dati cifrati da quelli di tracciamento con una probabilità sufficientemente elevata, rendendo così le attività di tracciamento non è rilevabili [24].

Nel periodo 2003-2005 ci siamo occupati di presentare una metodologia per la progettazione di modelli di simulazione di sistemi biologici che tengono conto del verificarsi di errori casuali e consentendo il rilevamento di tali errori tramite codici di Hamming [40,43].

Transazioni commerciali e crittografia

Una problematica, affrontata nel periodo 2006-2009, è stata quella dei documenti elettronici relativi a transazioni commerciali tra imprese internazionali, transazioni che da sempre si scontrano con l'assenza di precise normative che regolano scambio di dati. L'insieme di regole sviluppate dall'American National Standards Institute e dall'United Nations Economic Commission for Europe sancì, di fatto, la nascita di diversi standard per lo scambio di dati. In questo contesto, l'attività di ricerca svolta si è concentrata sullo studio degli standard esistenti, sulle problematiche inerenti alla sicurezza dei dati trasmessi in rete e sulle possibili contromisure da adottare attraverso l'uso di tecniche crittografiche. Tali tecniche sono le sole in grado di garantire la non contraffazione, l'autenticità e la firma di documenti digitali, prevenendo frodi informatiche basate sulla debolezza intrinseca del sistema di trasmissione adottato. L'attività di ricerca svolta ha portato alla pubblicazione dei seguenti lavori [12,33,34].

2.1.2 **Modelli per il riconoscimento delle intrusioni**

Sistemi immunitari artificiali

L'attività di ricerca svolta nel periodo 2004-2011 ha riguardato lo studio e l'ideazione di nuovi modelli computazionali che prendono spunto dal natural immune system secondo l'approccio del biologically motivated computing. Questi modelli computazionali si basano sul paradigma immunitario e sui rilevatori di intrusioni, di virus, di worm in sistemi distribuiti e non. Quello degli Artificial Immune Systems (AISs) è un paradigma di elaborazione dell'informazione ispirato alla biologia. Le sue principali caratteristiche fanno riferimento alle proprietà e al comportamento del sistema immunitario innato e adattivo, responsabili della protezione dell'organismo dagli attacchi di agenti esterni. Il sistema immunitario impiega una difesa multilivello contro gli antigeni e ha il suo punto di forza nell'adattabilità. Infatti, esso è in grado di riconoscere la presenza di nuovi antigeni e di attivare, proliferare e differenziare la risposta immunitaria. Queste caratteristiche rendono il sistema tollerante, flessibile e capace di interagire con l'ambiente circostante, ma possono anche generare situazioni pericolose nelle quali il sistema immunitario erroneamente attacca sé stesso. Le similitudini evidenziate tra il sistema immunitario biologico e la protezione delle reti di computer hanno portato all'ideazione, alla progettazione e allo sviluppo di un sistema immunitario artificiale principalmente utilizzato per il rilevamento delle intrusioni, di virus e di spam in reti di calcolatori. In particolare, l'attività di ricerca svolta si è focalizzata sulla necessità di definire una nuova metodologia per il riconoscimento di antigeni artificiali basata sulla logica fuzzy, cercando di minimizzare il numero di casi di autoimmunità. I risultati di questo lavoro di ricerca hanno portato alla pubblicazione dei seguenti articoli [11,13-15,25-32,35-39,41,42].

2.2 Pubblicazioni

ORCID: http://orcid.org/0000-0001-5689-8575
Scopus: https://www.scopus.com/authid/detail.uri?authorId=7006465120
Google Scholar: https://scholar.google.it/citations?hl=it&user=LPlGR5UAAAAJ

Journals

1. A.Visconti, F.Gorla, *Exploiting an HMAC-SHA-1 optimization to speed up PBKDF2*. IEEE Transactions on Dependable and Secure Computing, DOI: 10.1109/TDSC.2018.2878697, ISSN 1545-5971, in press.
2. A.De Piccoli, A.Visconti, O.G.Rizzo, *Polynomial multiplication over binary finite fields: new upper bounds* , Journal of Cryptographic Engineering, DOI: 10.1007/s13389-019-00210-w, ISSN 2190-8508, in press.
3. B.Bakree, M.Ceria, T.Moriarty, A.Visconti *Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures*, Applicable Algebra in Engineering, Communication and Computing, DOI: 10.1007/s00200-020-00428-w, ISSN 0938-1279, in press.
4. M. Raeiszadeh, H.Tahayori, A.Visconti, *Discovering varying patterns of Normal and interleaved ADLs in smart homes*. Applied Intelligence, 49(12), pg.4175-4188, ISSN 0924-669X, 2019.
5. A.Visconti, O.Mosnáček, M.Brož, V.Matyáš, *Examining PBKDF2 security margin --- case study of LUKS*, Journal of Information Security and Applications, 46, pg.296-306, ISSN 2214-2126, 2019.
6. D.G.V.Albricci, M.Ceria, F.Cioschi, N.Fornari, A.Shakiba, A.Visconti, *Measuring Performances of a White-Box Approach in the IoT Context*. Symmetry, 11(8), Article number 1000, ISSN 2073-8994, 2019.
7. M.Erfanmanesh, H.Tahayori, A.Visconti, *Elderly Action Prediction and Anomalous Activity Detection in Smart Homes through Profiling Residents' Behavior*. Modern Care Journal, 16(3), ISSN 2423-787, 2019.
8. A.Visconti, C.V.Schiavo, R.Peralta, *Improved upper bounds for the expected circuit complexity of dense systems of linear equations over GF(2)*. Information Processing Letters, 137, pg.1-5, ISSN 0020-0190, 2018.
9. L.Casati, A.Visconti, *The Dangers of Rooting: Data Leakage Detection in Android Application*. Mobile Information Systems, Article ID 6020461, ISSN 1574-017X, 2018.
10. G.Haus, C.Polizzi, A.Visconti, *Preserving cultural heritage: A new approach to increase the life expectancy of optical disc*. Journal of Cultural Heritage, 29, pg.67-74, ISSN 1296-2074, 2018.
11. A.Visconti, H.Tahayori, *Artificial immune system based on interval type-2 fuzzy set paradigm*. Applied Soft Computing, 11(6), pg.4055-4063, ISSN 1568-4946, 2011.
12. A.Pagnoni, A.Visconti, *Secure Electronic Bills of Lading: Blind Counts and Digital Signatures*. Electronic Commerce Research, 10(3), pg.363-388, ISSN 1389-5753, 2010.
13. A.Visconti, H.Tahayori, *A Biologically-Inspired Type-2 Fuzzy Set Based Algorithm for Detecting Misbehaving Nodes in Ad-Hoc Wireless Networks*. International Journal for Infonomics, 3(2), pg.373-382, ISSN 1742-4712, 2010.

14. H.Tahayori, A.G.B.Tettamanzi, G.Degli Antoni, A.Visconti, M.Moharrer, *Concave Type-2 Fuzzy Sets: Properties and Operations*. Soft Computing, 14(7), pg.749-756, ISSN 1432-7643, 2010.
15. H.Tahayori, A.G.B. Tettamanzi, G.Degli Antoni, A.Visconti, *On the Calculation of Extended Max and Min Operations between Convex Fuzzy Sets of the Real Line*. Fuzzy Sets and Systems, 160(21), pg.3103-3114, ISSN 0165-0114, 2009.

Conferences and book chapters

16. F.Cioschi, N.Fornari, A.Visconti, *White-box Cryptography: A Time-security Trade-off for the SPNbox Family*. In proceedings of the 2nd International Conference on International Conference on Wireless, Intelligent and Distributed Environment for Communication, WIDECOM 2019, I.Woungang, S.K.Dhurandher, Eds., ISSN 2367-4512, Lecture Notes on Data Engineering and Communications Technologies, Vol.27, Springer-Verlag, 2019.
17. A.F.Iuorio, A.Visconti, *Understanding Optimizations and Measuring Performances of PBKDF2*. In proceedings of the 2nd International Conference on International Conference on Wireless, Intelligent and Distributed Environment for Communication, WIDECOM 2019, I.Woungang, S.K.Dhurandher, Eds., ISSN 2367-4512, Lecture Notes on Data Engineering and Communications Technologies, Vol.27, Springer-Verlag, 2019.
18. M.Ceria, T.Mora, A.Visconti, *Efficient Computation of Squarefree Separator Polynomials*. In proceedings of the 6th International Conference on Mathematical Software, ICMS 2018, J.H.Davenport et al., Eds., LNCS 10931, ISSN 0302-9743, Springer-Verlag, 2018.
19. L.Casati, A.Visconti, *Exploiting a Bad User Practice to Retrieve Data Leakage on Android Password Managers*. In Advances in Intelligent Systems and Computing, 11th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2017, LNCS 612, ISSN 2194-5357, Springer-Verlag, 2017.
20. A.Visconti, S.Bossi, H.Ragab, A.Calo', *On the Weaknesses of PBKDF2*. In Cryptology and Network Security, 14th International Conference on Cryptology and Network Security, CANS 2015, LNCS 9476, ISSN 0302-9743, Springer-Verlag, 2015.
21. S.Bossi, A.Visconti, *What Users Should Know About Full Disk Encryption Based on LUKS*. In Cryptology and Network Security, 14th International Conference on Cryptology and Network Security, CANS 2015, LNCS 9476, ISSN 0302-9743, Springer-Verlag, 2015.
22. S.Mella, F.Melzani, A. Visconti, *Differential Fault Attacks against AES tampering with the Instruction Flow*. In proceedings of the 11th International Conference on Security and Cryptography, SECRYPT14, ISBN 978-9-8985-6595-2, 2014.
23. D.D'angella, C.V. Schiavo, A. Visconti, *Tight upper bounds for polynomial multiplication*. In proceedings of the 6th WSEAS world congress: applied computing conference, ACC '13, ISBN 9789604743544, 2013.
24. C.V. Schiavo, A. Visconti, *An improved public-key tracing scheme with sublinear ciphertext size*. In proceedings of the 9th International Conference on Security and Cryptography, SECRYPT12, ISBN 978-989-8565-24-2, 2012.
25. H.Tahayori, Alireza Sadeghian, Andrea Visconti *Operations on Type-2 Fuzzy Sets Based on the Set of Pseudo-Highest Intersection Points of Convex Fuzzy Sets*. In IEEE Proceedings of the 2010 Annual Meeting of the North American Fuzzy Information Processing Society, NAFIPS10, ISBN 978-1-4244-7857-6, 2010.

26. A.Visconti, H.Tahayori, *Detecting Misbehaving Nodes in MANET with an Artificial Immune System Based on Type-2 Fuzzy Sets*. In IEEE Proceedings of the 4th International Conference for Internet Technology and Secured Transactions, ICITST09, ISBN 978-1-4244-5647-5, 2009.

27. A.Visconti, H.Tahayori, *A Type-2 Fuzzy Set Recognition Algorithm for Artificial Immune Systems*. In Hybrid Artificial Intelligence Systems, 3rd International Workshop HAIS 2008, E.Corchado et al., Eds., LNCS 5271 (LNAI), ISSN 0302-9743, Springer-Verlag, 2008.

28. A.Visconti, N.Fusi, H.Tahayori, *Intrusion Detection via Artificial Immune System: a Performance-based Approach*. In Biologically-Inspired Collaborative Computing, IFIP 20th World Computer Congress, 2nd IFIP International Conference on Biologically-Inspired Collaborative Computing, M.Hinchey et al., Eds., Vol.268/2008, ISSN 1571-5736, Springer-Verlag, 2008.

29. H.Tahayori, A.Visconti, *Distributed-Interval Type-2 Fuzzy Set Based Recognition Algorithm for IDS*. In Proceedings of the 2008 IEEE International Conference on Granular Computing, GrC08, ISBN 978-1-4244-2512-9, 2008.

30. H.Tahayori, A.Visconti, G.Degli Antoni, *Spam Filtering Model Based on Interval Type-2 Fuzzy Set Paradigm*. In IEEE Proceedings of the 5th International Conference on Information & Communications Technology, ICICT07, ISBN 978-1-4244-1430-7, 2007.

31. H.Tahayori, A.Visconti, G.Degli Antoni, *Email Granulation Based On Distributed-Interval Type-2 Fuzzy Set Methodologies* In Proceedings of the 2007 IEEE International Conference on Granular Computing, GrC07, ISBN 0-7695-3032-X, 2007.

32. H.Tahayori, A.Visconti, G.Degli Antoni, *Augmented Interval Type-2 Fuzzy Set Methodologies for Email Granulation*. In Proceedings of the 2nd IEEE International Workshop on Soft Computing Applications, SOFA07, ISBN 978-1-4244-1608-0, 2007.

33. A.Visconti, *EZK: A Zero Knowledge Tool For Generating, Handling, And Securing Electronic Bills Of Lading*. In Proceedings of the 3rd International Conference on Web Information System and Technologies, WEBIST07, ISBN 978-972-8865-79-5, 2007.

34. A.Pagnoni, A.Visconti, *Electronic Bill of Lading: A Cryptographic Protocol*. In Proceedings of IADIS International Conference e-commerce 2006, ISBN 972-8924-23-2, 2006.

35. A.Pagnoni, A.Visconti, *Real-time Detection of Pathological Traffic Situations via AIS*. In Proceedings of Entwurf komplexer Automatisierungssysteme, E. Schnieder, ed., EKA06, ISBN 3-9803363-9-5, 2006.

36. A.Pagnoni, A.Visconti, *SIGNET: A Tool for Securing Complex Petri-Net Projects*. In Proceedings of Entwurf komplexer Automatisierungssysteme, E.Schnieder, ed., EKA06, ISBN 3-9803363-9-5, 2006.

37. A.Pagnoni, A.Visconti, *Profiling Network Attacks via AIS*. In Neural Nets, 16th Italian Workshop on Neural Nets, WIRN05, and International Workshop on Natural and Artificial Immune System, NAIS05, B.Apolloni et al., Eds., LNCS 3931, ISSN 0302-9743, Springer-Verlag, 2005.

38. A.Pagnoni, A.Visconti, *An Innate Immune System for the Protection of Computer Networks*. In Proceedings of the 4th International Symposium on Information and Communication Technologies, WISICT05, B.R.Baltes et al., eds., ACM International Conference Proceedings Series, ISBN 0-9544145-6-X, 2005.

39. A.Visconti, *Testing of Native Immune System for the Protection of Computer Networks*. In Proceedings of IADIS International Conference Applied Computing 2005, Vol. 2, ISBN 972-99353-6-X, 2005.

40. A.Pagnoni, A.Visconti, *Simulation of Error-Prone Biological Systems*. In Proceedings of the Winter International Symposium on Information and Communication Technologies, WISICT04, M.Alesky et al., eds., ACM International Conference Proceedings Series, ISBN 0-9544145-3-5, 2004.
41. A.Pagnoni, S.A.Parisi, A.Visconti, *Intrusion Detection via Artificial Immune Networks*. In Proceedings of X Convencion International y Feria INFORMATICA 2004, La Habana, Cuba, ISBN 959-237-227-2, 2004.
42. A.Pagnoni, A.Visconti, *NAIS: Intrusion Detection via Native Immune Systems*. In Communications, Information Technologies and Computing, Proceedings of the 10th International Conference on Cybernetics and Information Technologies, Systems and Applications, CITSA04, ISBN 980-6560-19-1, 2004.
43. A.Pagnoni, A.Visconti, *Detection and Analysis of Unexpected State Components in Biological Systems*. In Computational Methods in Computer Biology, 1st International Workshop, CMSB03, LNCS 2602, Springer-Verlag, ISSN 0302-9743, Springer-Verlag, 2003.

Altre pubblicazioni

44. A.Visconti, *Crittografia: tra successi e fallimenti*. DigitCult - Scientific Journal on Digital Cultures, 4(3), ISSN 2531-5994, 2019.
45. A.Visconti, *Block cipher*. 100 Tesi di crittografia e codici in Italia 2008-2017, Collana Crittografia, Book Series 3, Aracne, ISBN 978-88-255-2752-0, 2020.

2.3 Direzione o partecipazione alle attività di un gruppo di ricerca caratterizzato da collaborazioni a livello nazionale o internazionale

Visconti è stato responsabile e coordinatore delle attività del laboratorio di ricerca "Cryptography and Coding Laboratory (CLUB)" presso il Dipartimento di Informatica, Università degli studi di Milano dal 2009 al 2015 e, a seguito della fusione con il laboratorio di sicurezza LASER, dal 2015 è membro del "System Security and Cryptography Lab". Attualmente è il responsabile delle attività svolte dal gruppo di crittografia del lab stesso e supervisiona il lavoro di un post-doc e due dottorandi. Dal 2009 ad oggi, le principali collaborazioni nazionali e internazionali in ambito crittografico sono state quelle con i seguenti gruppi di ricerca:

- Computer Security Division - NIST;
- Centre for Research on Cryptography and Security - Masaryk University;
- Laboratorio di Matematica Industriale e Crittografia (CryptoLabTN) dell'Università degli Studi di Trento.

La collaborazione in ambito “high-speed cryptography” con il gruppo di crittografia dell’Information Technology Lab – Computer Security Division del NIST è stata supportata da un'attività di visiting ed è sfociata nella seguente pubblicazione:
https://www.nist.gov/publications/improved-upper-bounds-expected-circuit-complexity-dense-systems-linear-equations-over

La collaborazione in ambito “Key Derivation Functions e Disk Encryption” con il gruppo del Prof. V.Matyáš, Centre for Research on Cryptography and Security, Masaryk University è sfociata nella seguente pubblicazione:
https://www.sciencedirect.com/science/article/abs/pii/S221421261730025X

Collaborazione con i ricercatori del Laboratorio di Matematica Industriale e Crittografia (CryptoLabTN) dell'Università degli Studi di Trento nel progetto “Optimization of Groebner Basis

Computations for ECDLP (OGBC4EC)", progetto risultato vincitore della call CINECA Italian SuperComputing Resource Allocation (ISCRA).

2.3.1 Attività di supervisione di post-doc, dottorandi e assegnisti

Dal 2009 a oggi, Andrea Visconti ha supervisionato il lavoro di ricerca di:

- Michela Ceria (post-doc, da maggio 2018 a oggi)
- Alessandro De Piccoli (dottorando XXXIV Ciclo, da ottobre 2018 a oggi)
- Sergio Polese (dottorando XXXV Ciclo, da ottobre 2019 a oggi)
- Silvia Mella (dottorando XXIX Ciclo, da gennaio 2014 a dicembre 2014)
- Chiara Schiavo (dottorando XXVI Ciclo, da gennaio 2011 a ottobre 2014)

e gli incarichi di lavoro autonomo e occasionale di carattere intellettuale di:

- Cristian Lepore (contratto su progetto di ricerca, due mesi nel 2019)

2.3.2 Organizzazione di competizioni nazionali

Con l'obiettivo di promuovere la cultura della sicurezza, e far comprendere alla comunità scientifica che gli algoritmi crittografici devono essere continuamente testati, mantenuti e migliorati, Visconti è stato responsabile di due gare crittografiche nazionali: "Cryptowars 2019" e "Cryptowars 2018". Gli eventi, organizzati nell'ambito dell'ECSM (European Cyber Security Month) in collaborazione con la De Componendis Cifris (Associazione italiana di Crittografia) e il Clusit, hanno visto la partecipazione di squadre provenienti delle seguenti università italiane: Politecnico di Tornino, Università degli Studi di Torino, Università degli Studi di Perugia, Università degli Studi dell'Aquila, Università degli Studi di Trento, Università degli Studi di Cagliari, Università degli Studi di Milano-Bicocca, Università degli Studi Roma Tre e Università degli Studi di Milano.

Con l'obiettivo di sensibilizzare e incentivare coloro che desiderano programmare smart contracts in ambito blockchain, Visconti, in collaborazione con l'Associazione italiana di Crittografia, ha organizzato il "De Cifris Hackathon 2019", competizione a squadre di un giorno con montepremi di 6KEur.

2.4 Responsabilità scientifica per progetti di ricerca finanziati sulla base di bandi competitivi o commissionati da istituzioni pubbliche/private

- Principal Investigator del contratto commissionato "Analisi algebrica di HMAC-SHA-1". Durata 12 mesi, nel periodo 2019-oggi.
- Co-Principal Investigator del progetto di ricerca "Obiettivo immagine: Estetica della fotografia e cultura del territorio" e responsabile dell'unità di ricerca del Dipartimento di Informatica, Università degli Studi di Milano. Progetto biennale (2017-2019) vincitore di un bando Fondazione Cariplo. Il progetto ha come obiettivi la tutela dei diritti d'autore attraverso l'uso di avanzate tecniche crittografiche e la valorizzazione di nuovi talenti artistici. Finanziamento di 40kEUR.
- Principal Investigator del contratto commissionato "Scelta di opportuni algoritmi crittografici e la definizione dei rispettivi parametri di sicurezza da utilizzare nell'implementazione di un prototipo per la condivisione e la protezione di dati". Durata 3 mesi, nel 2019, finanziamento 5kEur.
- Principal Investigator del progetto di ricerca "Optimization of Groebner Basis Computations for ECDLP", progetto risultato vincitore della call CINECA Italian SuperComputing Resource Allocation (ISCRA) classe C. Durata 9 mesi, nel periodo 2017-2018.
- Principal Investigator del progetto "Analysis of Password-Based Key Derivation Functions" nel contesto del Piano di Sostegno alla Ricerca (PSR), Linea 2A, dell'Università degli Studi di Milano. Nel triennio 2015-2017, finanziamento di 8kEur.
- Co-Principal Investigator del contratto commissionato da Lombardia Informatica spa. Durata 8 mesi, nel periodo 2012-2013, finanziamento di 96kEur.

2.5 Organizzazione o partecipazione come relatore a convegni di carattere scientifico

- TPC Co-Chair dell'*International Conference on Wireless, Intelligent and Distributed Environment for COMmunication* (WIDECOM), 2020. https://tinyurl.com/ybelzde5
- General Co-Chair del workshop *Cryptanalysis: a key tool in securing and breaking ciphers* all'interno dell'Italian Conference on Cybersecurity (ITASEC), 2020.
- General Chair dell'*International Conference on Wireless, Intelligent and Distributed Environment for COMmunication* (WIDECOM), 2019. https://tinyurl.com/y2zhlwet
- Session Chair alla *11th International Conference on Security and Cryptography* (SECRYPT), 2014.

2.5.1 Membro del comitato di programma

- Program committee, International Conference on Emerging Security Information, Systems and Technologies (SECURWARE) dal 2020 al 2016.
- Program committee, International Conference on Advances in CyberSecurity (ACeS) 2020, 2019.
- Program committee, Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS) dal 2020 al 2018.
- Program committee, Future of Information and Communication Conference (FICC) dal 2020 al 2018.
- International conference on Parallel, Distributed Computing and Applications (IPDCA), 2020.
- Program Committee, Future Technologies Conference (FTC) dal 2020 al 2016.
- Program committee, International Conference on Networks & Communications (NWCOM) 2019.
- Program committee, Intelligent Systems Conference (IntelliSys) 2019, 2018, 2016.
- Program committee, International Conference on Advanced Computer Science and Information Technology (ICAIT) 2019.
- Program committee, International Conference Sciences of Electronics, Technologies Information and Telecommunications (SETIT) 2018.
- Program committee, International Symposium on Computer Science and Intelligent Control (ISCSIC) 2017.
- Program committee, International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS) 2012.

2.5.2 Invited speaker

- Invited speaker al PoliMI Fintech Journey 2018 "From Blockchain&Bitcoin to Distributed Ledger Technologies, Smart Contracts and Cryptocurrencies in Finance". Titolo dell'intervento: "On the cryptography of DLT" (https://www.mate.polimi.it/EKO/FINTECH/Program.pdf)
- Invited speaker al Sesto Workshop di Crittografia "BunnyTN6 2015". Titolo dell'intervento: "What users should know about Full Disk Encryption based on LUKS" (http://www.science.unitn.it/~sala/events2015/BunnyTN6.html)
- Invited speaker al Quarto Workshop di Crittografia "BunnyTN4 2013". Titolo dell'intervento: "Heuristics to minimize the complexity of digital circuits" (http://www.science.unitn.it/~sala/events2013/BunnyTN4.html)
- Invited speaker al Terzo Workshop di Crittografia "BunnyTN3 2012". Titolo dell'intervento: "Vulnerabilità dei protocolli SSL/TLS" (http://www.science.unitn.it/~sala/BunnyTN/index2012_march.html)

- Invited speaker alla X Convención International y Feria INFORMATICA 2004. Titolo dell'intervento "Intrusion Detection via Artificial Immune Networks"

2.5.3 Relatore a convegni di carattere scientifico

- Relatore alla 14th International Conference on Cryptology and Network Security, CANS 2015 e presentazione del paper "On the Weaknesses of PBKDF2"
- Relatore alla 14th International Conference on Cryptology and Network Security, CANS 2015 e presentazione del paper "What Users Should Know About Full Disk Encryption Based on LUKS"
- Relatore alla 11th International Conference on Security and Cryptography, SECRYPT 2014, e presentazione del paper "Differential Fault Attacks against AES tampering with the Instruction Flow"
- Relatore all'IFIP 20th World Computer Congress, Second IFIP TC 10 International Conference on Biologically-Inspired Collaborative Computing, e presentazione del paper "Intrusion Detection via Artificial Immune System: a Performance-based Approach"
- Relatore alla IADIS International Conference on e-Commerce e presentazione del paper "Electronic Bill of Lading: A Cryptographic Protocol"
- Relatore al 4th International Symposium on Information and Communication Technologies, WISICT 2005 e presentazione del paper "An Innate Immune System for the Protection of Computer Networks"
- Relatore alla 10th International Conference on Cybernetics and Information Technologies, Systems and Applications, CITSA 2004, e presentazione del paper "NAIS: Intrusion Detection via Native Immune Systems"
- Relatore al First International Workshop in Computational Methods in Systems Biology, CMSB 2003 e presentazione del paper "Detection and Analysis of Unexpected State Components in Biological Systems"

2.6 Partecipazione a comitati editoriali di riviste, collane editoriali ed enciclopedie

- Lead guest editor della special issue *Theoretical Aspects of Cryptography and Their Applications for Data Protection in Emerging 5G Systems*, Security and Communication Networks (Hindawi), 2019.
- Guest editor della special issue *Internet of Things: design, architectures and protocols*, Internet of Things (Elsevier), 2019.
- Associate Editor dell'Iran Journal of Computer Science (Springer), dal 2018 ad oggi.
- Membro del Comitato Scientifico della collana editoriale intitolata *Crittografia* (Aracne), dal 2017 ad oggi.
  (http://www.aracneeditrice.it/index.php/collana.html?col=CRY)
- Membro dell'Editorial Board, Open Journal of Information Security and Applications, ISSN: 2374-6262, dal 2014 al 2016.
  (https://tinyurl.com/y3utkrow)

2.6.1 Revisore per journal e conferenze internazionali

Visconti è, o è stato, revisore per:

- IEEE Transactions on Dependable and Secure Computing
- Communications of the ACM

- Journal of Cryptographic Engineering
- Journal of Computer Security
- Journal of Information Security and Applications
- SN Computer Science
- Journal of Systems and Software
- International Journal of Autonomous and Adaptive Communications Systems
- International Journal of Unconventional Computing
- IEEE Wireless Communications and Networking Conference (WCNC) 2016
- ASIACRYPT 2014
- WIRN 2014

3 ATTIVITÀ TERZA MISSIONE

3.1 Risultati ottenuti nel trasferimento tecnologico in termini di partecipazione alla creazione di nuove imprese

Andrea è co-founder dello spin-off dell'Università degli Studi di Milano "AuthclicK srl" e membro del CDA dello stesso. Authclick intende promuovere 1) la valorizzazione delle opere fotografiche; 2) la protezione dei diritti d'autore, e la loro gestione, attraverso tecniche crittografiche innovative; 3) mostre, esposizioni, eventi; 4) corsi di formazione anche in partnership con accademie, enti culturali, fondazioni, università e centri di ricerca. Il progetto ha ricevuto l'approvazione dei dipartimenti coinvolti nell'arco temporale luglio-ottobre 2018. Approvato dalla commissione brevetti nel novembre 2018 dal CDA di UniMi nel dicembre 2018. Costituzione di AuthclicK srl il 5.02.2019. Pagina web: https://authclick.net/

3.1.1 Premi e riconoscimenti

L'idea progettuale, che ha portato all'apertura della start up Authclick srl, è risultata:

- nel 2017, finalista alla Startcup Lombadia;
- nel 2018, vincitrice dell'iniziativa "Idee Vincenti" promossa da Lottomatica in collaborazione con il Polihub (Innovation District & Startup Accelerator del Politecnico di Milano). Lo scopo di tale iniziativa era quello di contribuire all'innovazione dei beni culturali puntando su tecnologia ed imprenditorialità. Riscontro di tale iniziativa lo si può trovare qui: Lottomatica, Polihub, Repubblica.

3.2 Relatore a convegni ed eventi di carattere divulgativo

- Intervento alla "Settimana Amministrazione Aperta" organizzato dal Ministero per le Attività Culturali e per il Turismo nel 2019;
  (https://tinyurl.com/ybgc3s3n)
- Intervento alla conferenza "Crittografia e Crittotecnologie: dalla cifratura delle informazioni segrete alle moderne applicazioni in ambito civile e militare" organizzata dall'Armed Forces Communications & Electronics Association (AFCEA) nel 2019;
  (https://tinyurl.com/ybxb5xar)
- Intervento all'evento "L'associazione De Cifris incontra Torino" organizzato dall'associazione De Cifris nel 2019;
  (https://crypto.polito.it/eventi/convegno_la_de_cifris_incontra_torino)
- Intervento all'evento "Milano Digital Week" iniziativa promossa dall'Assessorato a Trasformazione Digitale e Servizi Civici del Comune di Milano nel 2019;
  (http://milanodigitalweek.unimi.it/)
- Intervento al workshop "Blockchain, HSM e protezione dei dati" organizzato da Symbolic e Thales nel 2018;
  (https://tinyurl.com/yclm43bn)

- Intervento all'evento "CifrisChain 2018" organizzato dall'associazione De Cifris nel 2018; (https://www.decifris.it/index_dicembre2018.html)
- Intervento all'evento "L'associazione De Cifris incontra Milano" organizzato dall'associazione De Cifris nel 2018; (https://www.unimib.it/eventi/lassociazione-de-cifris-incontra-milano)
- Intervento al workshop "Competenze digitali per lo sviluppo dell'economia Italiana, sviluppo delle competenze digitali in Italia" organizzato da Confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa nel 2015; (https://tinyurl.com/y6vmv57q)

4 ATTIVITÀ DIDATTICHE

4.1 Corsi per laurea magistrale, specialistica e triennale

A.A. 2019/20
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Matematica, Laboratorio di Programmazione 1, 36 ore.

A.A. 2018/19
- Università degli Studi di Milano - Corso di laurea in Informatica, Teoria dell'Informazione e della Trasmissione, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.

A.A. 2017/18
- Università degli Studi di Trento - Corso di laurea in Matematica, Advanced Programming of Cryptographic Methods, 35 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Teoria dell'Informazione e della Trasmissione, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.

A.A. 2016/17
- Università degli Studi di Trento - Corso di laurea in Matematica, Advanced Programming of Cryptographic Methods, 35 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia Avanzata, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.

A.A. 2015/16
- Università degli Studi di Trento - Corso di laurea in Matematica, Advanced Programming of Cryptographic Methods, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia Avanzata, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.

A.A. 2014/15
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia Avanzata, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.

A.A. 2013/14
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.

- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 2, 48 ore.

A.A. 2012/13
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 2, 48 ore.

A.A. 2011/12
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 2, 48 ore.

A.A. 2010/11
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.

A.A. 2009/10
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia 1, 48 ore.

A.A. 2008/09
- Università degli Studi di Milano - Corso di laurea in Informatica per le Telecomunicazioni, Teoria dell'Informazione e della Trasmissione, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Chimica e Tecnologia Farmaceutiche, Abilità Informatiche, 36 ore.
- Università degli Studi di Milano - Corso di laurea in Scienze Biologiche, Laboratorio di Informatica, 32 ore.

A.A. 2007/08
- Università degli Studi di Milano - Corso di laurea in Informatica per le Telecomunicazioni, Teoria dell'Informazione e della Trasmissione, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Scienze Biologiche, Laboratorio di Informatica, 32 ore.

A.A. 2006/07
- Università degli Studi di Milano - Corso di laurea in Informatica per le Telecomunicazioni, Teoria dell'Informazione e della Trasmissione, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Scienze Biologiche, Laboratorio di Informatica, 32 ore.

A.A. 2005/06
- Università degli Studi dell'Insubria - Corso di laurea in Informatica, Algoritmi e Strutture Dati II, 48 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica. Attività di tutorato per il corso di Teoria dei Codici.
- Università degli Studi di Milano - Corso di laurea in Informatica. Attività di tutorato per il corso di Crittografia.

A.A. 2004/05
- Università degli Studi di Milano - Corso di laurea in Informatica, Teoria dei Codici, 24 ore.
- Università degli Studi di Milano - Corso di laurea in Informatica, Crittografia, 48 ore.

A.A. 2003/04
- Università degli Studi di Milano - Corso di laurea in Informatica. Attività di tutorato per il corso di Teoria dell'Informazione.
- Università degli Studi di Milano - Corso di laurea in Informatica. Attività di tutorato per il corso di Crittografia.

A.A. 2002/03

- Università degli Studi di Milano - Corso di laurea in Informatica. Attività di tutorato per il corso di Teoria dell'Informazione.
- Università degli Studi di Milano - Corso di laurea in Informatica. Attività di tutorato per il corso di Crittografia.

A.A. 2001/02

- Università degli Studi di Milano - Corso di laurea in Informatica. Attività di tutorato per il corso di Teoria dell'Informazione.
- Università degli Studi di Milano - Corso di laurea in Biotecnologie. Attività di tutorato per il corso di Informatica.

4.2 Percorsi formativi post-laurea

A.A. 2019/20

- Corso di perfezionamento intitolato “Innovazione tecnologica, nuovi mercati e regole. Piattaforme, blockchain, fintech e utente digitale” dell’Università degli Studi di Milano. Attività didattica del modulo “Blockchain: profili tecnici”, 2 ore.

A.A. 2003/04

- Master in “Sicurezza dell'Informazione e della Comunicazione” dell’Università degli Studi di Milano. Attività di tutorato per il corso di Crittografia, 18 ore.

A.A. 2001/02

- Master in “Metodologie di Base dell'Informatica per Umanisti” dell'Università degli Studi di Milano. Attività di tutorato per il corso di Programmazione, 18 ore.

4.3 Formale attribuzione di incarichi di insegnamento affidati da qualificati istituti nazionali o internazionali

- Scuola di formazione del Sistema di informazione per la Sicurezza della Repubblica, Presidenza del Consiglio dei Ministri, attività didattica in ambito crittografico, nel 2019, 1 settimana.
- Scuola di formazione del Sistema di informazione per la Sicurezza della Repubblica, Presidenza del Consiglio dei Ministri, attività didattica in ambito crittografico, nel 2017, 4 ore.
- Scuola di formazione del Sistema di informazione per la Sicurezza della Repubblica, Presidenza del Consiglio dei Ministri, attività didattica in ambito crittografico, nel 2015, 20 ore.
- Scuola di formazione del Sistema di informazione per la Sicurezza della Repubblica, Presidenza del Consiglio dei Ministri, attività didattica in ambito crittografico, nel 2014, 20 ore.

4.4 Lavori di tesi supervisionati

Andrea Visconti è stato relatore/correlatore di 96 tesi magistrali, specialistiche o triennali nei corsi di laurea di Informatica, Matematica, Fisica, Finance and economics presso l'Università degli Studi di Milano (UniMI), l'Università degli Studi di Trento (UniTN) e l'Università degli Studi di Padova (UniPD).

Relatore delle seguenti tesi presso UniMI

	Studente	Titolo Tesi	A.A.
1	CASATI LUCA	STUDIO, ANALISI E TESTING DI ALGORITMI CRITTOGRAFICI IMPLEMENTATI IN AMBITO IOT	2018/19
2	TIZIANI MARTINO	ANALISI E OTTIMIZZAZIONE DI UN'IMPLEMENTAZIONE SOFTWARE DI MCELIECE	2018/19
3	BONFANTI DANIELE	ANALISI E TESTING DELLE PERFORMANCE DI UN CIFRARIO RSA-LIKE	2018/19
4	CALCAGNI PAOLO	ANALISI DELLA BLOCKCHAIN DI MONERO E SUE POSSIBILI APPLICAZIONI AL PROTOCOLLO DI VOTO ELETTRONICO	2018/19
5	CASATI ILARIA	MCELIECE CRYPTOSYSTEM: ALGEBRAIC OPTIMIZATIONS OF A QUANTUM-RESISTANT CRYPTOGRAPHIC ALGORITHM	2018/19
6	ALBRICCI DANIELE GIACOMO VITTORIO	COAP E MQTT: ANALISI E TESTING DI DUE PROTOCOLLI IN AMBITO IOT	2018/19
7	BACCAINI FEDERICO	ANALISI E TESTING DELLA BLOCKCHAIN NEM	2018/19
8	CELORA CHRISTIAN	LEX GAME ITERATIVO TRAMITE BAR CODES E POLINOMI SEPARATORI PER LO STUDIO DI CONFIGURAZIONI FINITE DI PUNTI	2018/19
9	GARAVAGLIA SAMUELE	CRITTOANALISI DIFFERENZIALE DI UN CIFRARIO LIGHTWEIGHT	2018/19
10	HAMMAR YOUSEF	LUKS: STUDIO E ANALISI DELLE CRITICITA' DEL SISTEMA DI CIFRATURA DEI DISCHI	2018/19
11	MANNINO MIRKO	ANALISI PRESTAZIONALE DI SAT SOLVER PER VALUTAZIONE DI FUNZIONI CRITTOGRAFICHE	2018/19
12	MARCHESI LUCA	STUDIO E IMPLEMENTAZIONE DI TECNICHE DI CRITTOANALISI ALGEBRICA SU HMAC	2018/19
13	NEGRI MATTEO	IMPLEMENTAZIONE ED ANALISI DI UN CIFRARIO A BLOCCHI LIGHTWEIGHT	2018/19
14	PAOLINO MATTIA	ANALISI DI SPHINCS: PROPOSTA POST-QUANTUM PER FIRMA DIGITALE	2018/19
15	PAPALUCA GIACOMO	IMPLEMENTAZIONE E TESTING DI PRIMITIVE CRITTOGRAFICHE APPLICATE A MOSQUITTO, MQTT BROKER.	2018/19
16	PAPPAROTTO LUCA	BLOCKCHAIN E FOTOGRAFIA: CONNUBIO PERFETTO TRA CRITTOGRAFIA E ARTE	2018/19
17	QUAGLIARELLA GABRIELE	ARGON2 E LUKS: ANALISI CRITICA DI UNA IMPLEMENTAZIONE BASATA SU FUNZIONI CRITTOGRAFICHE MEMORY-HARD	2018/19
18	SHAKIBA ARVIN	IOT: ANALISI DI PROTOCOLLI DI COMUNICAZIONE PUBLISH/SUBSCRIBE	2018/19
19	TIRONE ANTONIO	ANALISI DELLE PERFORMANCE DI CIFRARI SOTTOPOSTI ALLA GARA POST-QUANTUM CRYPTOGRAPHY	2018/19
20	LEPORE CRISTIAN	COMPARATIVE ANALYSIS OF THE CRYPTOGRAPHIC SCHEMES IMPLEMENTED IN SEVERAL BLOCKCHAINS AND ALGORAND ANALYSIS.	2018/19
21	CIOSCHI FEDERICO	WHITE-BOX CRYPTOGRAPHY: UNA NUOVA PROPOSTA PER LA FAMIGLIA DI CIFRARI SPNBOX	2017/18
22	RIVA LORENZO	POST-QUANTUM CRYPTOGRAPHY: ANALISI DELLE PROPOSTE	2017/18
23	ROSSI LORENZO	BLOCKCHAIN AMBITI DI UTILIZZO ALTERNATIVI ALLE CRIPTOVALUTE	2017/18
24	CASATI LUCA	HOW TO DETECT INFORMATION LEAKAGE: A MOBILE APP SECURITY TESTING	2016/17
25	FERRETTI ANDREA	STUDIO E IMPLEMENTAZIONE DI UNA LIBRERIA CRITTOGRAFICA PER ATTACCHI ALGEBRICI	2016/17
26	GRIMI RICCARDO	GLI SVILUPPI DELLA BLOCKCHAIN: STUDIO E IMPLEMENTAZIONE DI SMART CONTRACT	2016/17
27	IVAN ALEXANDRU EMILIAN	PROPOSAL OF A NEW LIGHTWEIGHT HASH FUNCTION FOR CONSTRAINED DEVICES	2016/17
28	MAGGI FEDERICO	BEHAVIOURAL ANDROID MALWARE DETECTION THROUGH PATTERN MATCHING STRATEGIES	2016/17
29	MAURI MARCO	ANALISI CRITICA DEI PROTOCOLLI DI AUTENTICAZIONE DELLE APPLICAZIONI ANDROID IN SPECIFICI CONTESTI DI UTILIZZO	2016/17
30	TANSINI LUCA	IMPLEMENTAZIONE E TESTING DI TECNICHE DI CRITTOANALISI DIFFERENZIALE PER L'ALGORITMO DI KECCAK	2016/17
31	TIZIANI MARTINO	OTTIMIZZAZIONE DELLE PERFORMANCE DI UNA LIBRERIA CRITTOGRAFICA PER ATTACCHI ALGEBRICI	2016/17

32	INTORRE GIOVANNI	STUDIO E TESTING DI PROTOCOLLI DI AUTORIZZAZIONE IN DISPOSITIVI CON PRIVILEGI DI ROOT	2016/17
33	IUORIO ANDREA FRANCESCO	EXPLOITING SHA-1 WEAKNESSES TO SPEED UP PBKDF2	2016/17
34	SABBATINI PEVERIERI MATTEO	AN ELLIPTIC CURVE VERSION OF BRANDS' DIGITAL CASH SCHEME	2016/17
35	PICETTI FEDERICO	BLOCKCHAIN E SCHEMI CRITTOGRAFICI PER LA PROTEZIONE DEI DATI	2015/16
36	FORTE FEDERICO	ANALYSIS OF ANDROID OS: DATA LEAKAGE THROUGH MOBILE APPS	2015/16
37	GIORDANI DANILO	ANALISI DELLA SICUREZZA DI APPLICAZIONI MOBILI	2015/16
38	MERATI FRANCESCO	ANALISI E TESTING DI KEY DERIVATION FUNCTIONS PER LA GENERAZIONE DI PASSWORD CRITTOGRAFICAMENTE SICURE	2015/16
39	ROSSI STEFANO	TECNICHE DI MINIMIZZAZIONE CIRCUITALE E APPLICAZIONI IN AMBITO CRITTOGRAFICO	2015/16
40	GORLA FEDERICO	ANALISI E TESTING DI KDFS PER LA GENERAZIONE DI CHIAVI CRITTOGRAFICAMENTE SICURE	2015/16
41	BRIVIO RAFFAELE	ANALISI E TESTING DI PRIMITIVE CRITTOGRAFICHE PER LA GENERAZIONE DI DISCHI CIFRATI SU SISTEMI OPERATIVI UNIX-LIKE	2015/16
42	BERTANI DARIO EMILIO	INTRODUZIONE ALLA CAESAR COMPETITION PER LA DEFINIZIONE DI UN NUOVO AUTHENTICATED-ENCRYPTION SCHEME	2014/15
43	BONASSI NICOLA	PKI: MODELLO, APPLICAZIONI, VULNERABILITA' E CONTROMISURE	2014/15
44	BRESHANAJ ANDI	STUDIO, ANALISI E TESTING DELLA KEY DERIVATION FUNCTION SCRYPT	2014/15
45	CEFFA FILIPPO	ANALYSIS, IMPLEMENTATION AND TESTING OF KECCAK, THE WINNER OF THE SHA-3 COMPETITION	2014/15
46	MARANCINA DANIELE	TEST DI PRIMALITA': STUDIO E COMPARAZIONE DEGLI ALGORITMI UTILIZZATI PER LA GENERAZIONE DI CHIAVI SICURE	2014/15
47	NAITANA ANDREA	SALSA20, UN CIFRARIO A FLUSSO PER LE KDF	2014/15
48	PASCAZIO DAVIDE	ANALISI E IMPLEMENTAZIONE DI UNA PUBLIC KEY INFRASTRUCTURE	2014/15
49	ROSSI LORENZO	ANALISI CRITICA DEI CIFRARI SIMON E SPECK	2014/15
50	RENOLDI LAURA	IMPLEMENTAZIONE E TESTING DI UN DISTINGUISHER ATTACK PER CIFRARI A BLOCCHI	2014/15
51	BOSSI SIMONE	CAN A FDE SOLUTION PROVIDE SECURITY IN THE EVENT THAT PERSONAL DATA IS LOST OR STOLEN?	2013/14
52	RAGAB HANY	A KEY RECOVERY ATTACK ON SIX ROUNDS OF AES	2013/14
53	DI RIZZO CARLO	LE PROMETTENTI MONETE DIGITALI: UN'ANALISI CRITICA	2013/14
54	CAPRARO WILIAM	HEURISTICS FOR BOOLEAN CIRCUIT MINIMIZATION AND THEIR APPLICATIONS TO LIGHTWEIGHT CRYPTOGRAPHY	2013/14
55	MAZZIOTTI LUCA	ENCRYPTION SCHEMES IN CELLULAR NETWORKS	2012/13
56	TARTARINI YARI	STUDIO E TESTING DEGLI ALGORITMI CRITTOGRAFICI UTILIZZATI IN AMBITO BLUETOOTH	2012/13
57	CRISTALLI STEFANO	SECURITY IN REAL-TIME OPERATING SYSTEMS FOR MICROCONTROLLERS: A CASE STUDY ON FREERTOS.	2012/13
58	GORLA FEDERICO	ANALISI E TESTING DEI PROTOCOLLI DI AUTENTICAZIONE IMPLEMENTATI DALLA CNS	2012/13
59	PIZZIMENTI SIMONE	STUDIO, ANALISI E TESTING DI ALGORITMI CRITTOGRAFICI IMPLEMENTATI NEI SISTEMI OPERATIVI PER DISPOSITIVI MOBILI	2012/13
60	BURATTI DANIELE	STUDIO E ANALISI DEGLI ASPETTI DI SICUREZZA DELLE COMUNICAZIONI MOBILE COINVOLTE NEI PROTOCOLLI CRITTOGRAFICI DI AUTENTICAZIONE.	2012/13
61	PALMULLI LUCA	AES: STUDIO E IMPLEMENTAZIONE DELLO SQUARE ATTACK	2012/13
62	ZITO MATTIA	ANALISI DELLE TECNICHE CRITTOGRAFICHE IMPLEMENTATE NEL SERVIZIO DI VERBALIZZAZIONE ONLINE DEGLI ESAMI	2012/13
63	CARIOTI DIANA	STUDIO ED ANALISI DEI METODI DI AUTENTICAZIONE COMUNEMENTE UTILIZZATI	2011/12
64	LONGFILS GIULIO	PARALLELIZZAZIONE DI CODICE CRITTOGRAFICO PER LA GENERAZIONE DI 'BUONI' CIRCUITI SU GF(2)	2011/12
65	D'ANGELLA DAVIDE	STUDIO ED IMPLEMENTAZIONE DI ALGORITMI EFFICIENTI PER IL CALCOLO DELLA MOLTIPLICAZIONE POLINOMIALE IN SISTEMI CRITTOGRAFICI	2011/12
66	DE VAL FEDERICA	ANALISI E TESTING DELLE POPRIETA' DI CASUALITA' NEL PROCESSO DI GENERAZIONE DELLE CHIAVI PUBBLICHE	2011/12
67	CALVI LEONARDO ANDREA	ANALISI DELLA RANDOMICITA' DI SEQUENZE DI BIT PSEUDOCASUALI.	2011/12
68	BERNASCONI MARCO	SCRIVERE CODICE SICURO PER PREVENIRE ERRORI NOTI: ANALISI A POSTERIORI DI UN CASO REALE	2011/12
69	ASTOLFI LUCA	IMPLEMENTAZIONE DI ATTACCHI CRITTOGRAFICI PER VERIFICARE POSSIBILI DEBOLEZZE NELLA CRS	2010/11
70	CALLIGARI ERIK	CARTA REGIONALE DEI SERVIZI: ANALISI E TESTING DELLE FUNZIONI CRITTOGRAFICHE IMPLEMENTATE	2010/11

71	VERGA FEDERICO	RESISTENZA DELLE LIBRERIE CRITTTOGRAFICHE AL 'TIMING ATTACK'	2010/11
72	ALIPRANDI DIEGO	STUDIO E IMPLEMENTAZIONE DEL PROTOCOLLO CRITTOGRAFICO DELLA AACS PER LA PROTEZIONE DEL DIRITTO D'AUTORE	2010/11
73	ESPOSITO STEFANO	STUDIO E IMPLEMENTAZIONE DEI CODICI DI REED-SOLOMON PER LA RILEVAZIONE E LA CORREZIONE DELL'ERRORE.	2010/11
74	INTORRE GIOVANNI	ANALISI CRITICA DELL'ALGORITMO CRITTOGRAFICO CAMELLIA	2010/11
75	COLOMBO ROBERTA	ANALISI DELLE TECNICHE CRITTOGRAFICHE UTILIZZATE NELLA CARTA REGIONALE DEI SERVIZI	2009/10
76	FUMAGALLI MATTEO	DES IMPLEMENTAZIONE DELL'ATTACCO BASATO SU CRITTOANALISI DIFFERENZIALE	2009/10
77	QUAGGIA ANDREA	TECNICHE DI TRAITOR TRACING PER LA DIFESA DI MATERIALE PROTETTO	2009/10
78	BOCCHI MATTEO	IMPROVING THE PERFORMANCE OF A METHODOLOGY BY BOYAR JOAN AND PERALTA RENE FOR SIMPLIFICATION OF LINEAR FUNCTIONS BY ADDRESSING BOTH ITS CONSTRAINTS AND IMPLEMENTATION	2009/10
79	CASAGRANDE ALESSIO	RSA IMPLEMENTAZIONE DEL TIMING ATTACK	2009/10
80	MIRESSI FRANCESCO	STUDIO ED IMPLEMENTAZIONE DI UN FILTRO BASATO SU TYPE-2 FUZZY SET PER PIATTAFORME ANDROID	2009/10
81	RIMOLDI ANDREA	SICUREZZA NEI SISTEMI DI PAGAMENTO ELETTRONICO	2009/10
82	FRANK MARCO	DRM E METODI CRITTOGRAFICI COINVOLTI - RASSEGNA CRITICA	2008/09
83	FUSI NICOLO'	UN SISTEMA IMMUNITARIO ARTIFICIALE PER L'INTRUSION DETECTION BASATO SULL'ANALISI DELLE PRESTAZIONI	2006/07

Correlatore delle seguenti tesi presso UniMI

	Studente	Titolo Tesi	A.A.
84	POLIDORI GIULIA	BLOCKCHAIN TECHNOLOGY AND PUBLIC SECTOR	2018/19
85	DE PICCOLI ALESSANDRO	CRITTOGRAFIA HIGH-SPEED: NUOVI RISULTATI	2017/18
86	GARZIA CHIARA	HIGH-SPEED SOFTWARE IMPLEMENTATIONS OF ELLIPTIC CURVES	2015/16
87	CEFFA FILIPPO	ANALYSIS, IMPLEMENTATION AND TESTING OF KECCAK, THE WINNER OF THE SHA-3 COMPETITION	2014/15
88	CRISTALLI STEFANO	MEMORY TRACING TECHNIQUES FOR DEFEATING SPRAYING ATTACKS	2014/15
89	GIOFFRE' CLAUDIO	TECNICHE DI CANCELLAZIONE E RECUPERO DI DATI	2009/10
90	POLO PIERPAOLO	ZCASH STUDIO E IMPLEMENTAZIONE DI UN SISTEMA E-CASH CON PROTOCOLLI ZERO-KNOWLEDGE	2009/10
91	SCHIAVO CHIARA VALENTINA	RANDOMIZZAZIONE DI CHIAVI CRITTOGRAFICHE MEDIANTE FUNZIONI HASH: UN PROTOTIPO	2009/10
92	MILANESE DAVIDE	DOCUMENTI DI TRASPORTO ELETTRONICI SICURI: E-BOL BASATE SU PROTOCOLLI ZERO-KNOWLEDGE	2006/07
93	COPPOLA FRANCESCO ALBERTO	BILL OF LADING EDI, UN APPLICATIVO ZERO-KNOWLEDGE	2005/06

Relatore o correlatore delle seguenti tesi presso UniTN

	Studente	Titolo Tesi	A.A.
94	TAGLIARO CARLOTTA	SECURITY AND PERFORMANCE TRADEOFFS IN THE INTERNET OF THINGS	2018/19
95	MAGAGNA ANDREA	IOTA PROTOCOL: ANALYSIS AND TESTING OF THE SIGNATURE SCHEME	2017/18

Co-examiner delle seguenti tesi presso UniPD

	Studente	Titolo Tesi	A.A.
96	BERTO FILIPPO	NAMED DATA NETWORKING CONTENT POPULARITY PREDICTION AND APPLICATIONS	2019/20

4.5 Seminari tenuti presso istituti di ricerca nazionali o internazionali

- Seminario intitolato “SSL/TLS cryptographic protocols and their weaknesses” presso Dipartimento di Matematica e Fisica, Universtà Roma Tre, 2020;
- Seminario intitolato “Key derivation function: an essential (and usually transparent) component of real-world applications” presso Dipartimento di Matematica, Università degli Studi di Torino, 2019;
- Seminario intitolato “Applied cryptography and blockchain technology: an example of a notary service”, seminario organizzato da Fondazione Bruno Kessler e Dipartimento di Matematica, Universtà degli Studi di Trento, 2018;
- Seminario intitolato “Mobile Devices: How to Protect Sensitive Data” presso Dipartimento di Matematica, Universtà degli Studi di Trento, 2017;
- Seminario intitolato “Overview of SSL/TLS Encryption” all’interno del corso “Applications of Cryptography to Security and Privacy” dell’European Institute of Innovation and Technology (EIT), 2015;
- Seminario intitolato “IoT: Infrastrutture intelligenti e sicurezza” all’interno del corso “Information and Communication Technology” alla Libera Università di Lingue e Comunicazione IULM, 2015;
- Seminario intitolato “Vulnerabilità dei protocolli SSL/TLS” all’interno del corso “Applied Cryptography” dell’European Institute of Innovation and Technology (EIT), 2014;

5 Attività di servizio

- Membro della Commissione Esaminatrice per l’ammissione al Dottorato in Informatica per il XXXV ciclo, 2019.
- Membro della Commissione Orientamento in Ingresso, Dipartimento di Informatica, Università degli Studi di Milano, dal 2007–oggi.
- Membro della Giunta di Dipartimento nel ruolo di rappresentante dei ricercatori, Università degli Studi di Milano, dal 2015-oggi.
- Membro del Comitato di Direzione di Facoltà di Scienze e Tecnologie, Università degli Studi di Milano, dal 2015-oggi.
- Membro del Collegio Docenti della Scuola di Dottorato in Informatica, Università degli Studi di Milano, dal 2011 al 2017.
- Presidente di commissione per una procedura di valutazione per il conferimento di un incarico di collaborazione per l’attività di supporto alla ricerca nell’ambito del Progetto “Obiettivo immagine: estetica della fotografia e cultura del territorio”, 2019.

Data	14/09/2020	Luogo	Milano