Vincenzo Botta

ESPERIENZA LAVORATIVA

08/04/2024 – ATTUALE Roma
POST-DOC UNIVERSITA LA SAPIENZA DI ROMA

Ho un assegno di ricerca presso l'università La Sapienza di Roma e mi occupo di ricerca in ambito crittografico ed applicazioni di tecnologie crittografiche alle Blockchain sotto la supervisione del professor Daniele Venturi.

01/12/2022 – 31/03/2024 Varsavia, Polonia
POST-DOC UNIVERSITÀ DI VARSAVIA

Dal primo dicembre 2022 fino al 31 marzo 2024 sono stato un post-doc presso l'Università di Varsavia. Ho fatto ricerca in ambito crittografico ed applicazioni di tecnologie crittografiche alle Blockchain presso l'Università di Varsavia sotto la supervisione del professor Stefan Dziembowski.

01/10/2023 – 28/02/2024 Varsavia, Polonia
LECTURER UNIVERSITÀ DI VARSAVIA

Da ottobre 2023 sono stato il coordinatore ed il lecturer del corso "Introduction to Zero Knowledge" presso la facoltà di matematica, informatica e meccanica dell'università di Varsavia. Il corso si è tenuto per studenti di master. Il link alla pagina del corso è https://usosweb.mimuw.edu.pl/kontroler.php?_action=katalog2/przedmioty/pokazPrzedmiot&prz_kod=1000-2M23IZK

01/12/2021 – 30/11/2022 Fisciano, Italia
POST-DOC UNIVERSITÀ DEGLI STUDI DI SALERNO

Dal primo dicembre fino al 30 novembre 2022 sono stato un post-doc presso l'Università degli Studi di Salerno. Ho fatto ricerca in ambito crittografico ed applicazioni di tecnologie crittografiche alle Blockchain presso l'Università degli Studi di Salerno sotto la supervisione del professor Ivan Visconti.

01/12/2018 – 28/02/2022 Fisciano, Italia
STUDENTE DI DOTTORATO UNIVERSITÀ DEGLI STUDI DI SALERNO

Titolo della tesi: Security Enhancing Protocols for Data Protection and Distributed Computations.
Dal primo dicembre 2018 ho iniziato il percorso di dottorato presso il Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata (DIEM) dell'Università degli Studi di Salerno. Il tutor che ha seguito il mio percorso è il professor Ivan Visconti. Il tema di ricerca svolto durante il dottorato è lo studio di protocolli crittografici da applicare alla tecnologia Blockchain per ottenere la privacy dei dati col fine ultimo di soddisfare le esigenze delle applicazioni industriali.

- La borsa di dottorato vinta è stata finanziata dal POR CAMPANIA FSE 2014/2020 -DOTTORATI DI RICERCA CON CARATTERIZZAZIONE INDUSTRIALE DECRETO DIRIGENZIALE N. 155 DEL 17 MAGGIO 2018.
- 18 mesi del periodo di dottorato sono stati spesi presso l'Università degli Studi di Salerno. In questo periodo, sotto la supervisione del Prof. Ivan Visconti ho iniziato lo studio degli strumenti crittografici ed ho acquisito familiarità con le tecnologie blockchain.
- 12 mesi del periodo di dottorato sono stati spesi presso l'azienda Bit4Id di Napoli, presso cui sono stato coinvolto nelle attività di ricerca e sviluppo sulla tecnologia Blockchain. Presso l'azienda la mia attività è stata co-supervisionata dall'Ing. Paolo Campegiani.
- 6 mesi del periodo di dottorato sono stati spesi presso il gruppo di crittografia del dipartimento di informatica della Aarhus University, Danimarca. In questo periodo ho collaborato col gruppo di ricerca in tematiche relative alle blockchain. Presso la Aarhus University la mia attività è stata co-supervisionata dal Prof. Ivan Damgård.

28/12/2016 – 10/11/2018 Roma, Italia
INGEGNERE DEL SOFTWARE ACCELIZE ITALIA

Dal 28 dicembre 2016 ho svolto attività di verifica e validazione di un prodotto di Accelize Italia. La società si occupa di creazione di tool ed infrastrutture per la generazione di acceleratori per FPGA.

03/10/2016 – 07/12/2016 Roma, Italia

STAGE FORMATIVO EVERIS ITALIA

Ho seguito uno stage formativo presso la società Everis Italia dal 3 ottobre 2016 fino al 7 dicembre 2016. Lo scopo formativo di tale corso era di introdurmi alle tecnologie relative ai CRM, con particolare attenzione al tool CRMDynamics e di studiare le tecnologie utili per personalizzare tale tool per le diverse esigenze che posso esservi.

ISTRUZIONE E FORMAZIONE

09/2014 – 10/2016 Roma, Italia

LAUREA MAGISTRALE IN INFORMATICA La Sapienza Università di Roma

LM (DM 270/04) laurea di secondo livello in Informatica seguendo il curriculum di Ingegneria del Software.
La Sapienza Università di Roma - Facoltà di INGEGNERIA DELL'INFORMAZIONE, INFORMATICA E STATISTICA
-Livello: laurea di secondo livello (2 anni)
-Votazione finale: 110/110 e lode
-Media dei voti : 29.69
-Titolo della tesi: Alcuni risultati sulla complessità delle dimostrazioni in Risoluzione mediante una misura informazionale
-Soggetto della tesi: complessità delle dimostrazioni | Tipo di tesi: teorica

Campo di studio informatica | **Voto finale** 110 e lode/110 |

Tesi Alcuni risultati sulla complessità delle dimostrazioni in Risoluzione mediante una misura informazionale

09/2010 – 07/2014 Roma, Italia

LAUREA TRIENNALE IN INFORMATICA La Sapienza Università di Roma

L-31 laurea di primo livello in informatica
La Sapienza Università di Roma - Facoltà di INGEGNERIA DELL'INFORMAZIONE, INFORMATICA E STATISTICA
-Livello : laurea di primo livello (3 anni)
-Votazione finale : 106/110
-Media dei voti : 26.75
-Titolo della tes i: A survey of Lambda Expression in Java 8
-Soggetto della tesi : Linguaggi di programmazione | Tipo di tesi: teorica

Campo di studio Informatica | **Voto finale** 106/110 | **Tesi** A survey of Lambda Expression in Java 8

COMPETENZE LINGUISTICHE

Lingua madre: **ITALIANO**

Altre lingue: **INGLESE**

PUBBLICAZIONI

2025

Compact Proofs of Partial Knowledge for Overlapping CNF Formulae.

Avitabile, G., Botta, V., Friolo, D., Venturi, D., Visconti, I. 2025, Compact Proofs of Partial Knowledge for Overlapping CNF Formulae, Journal of Cryptology, vol. 38, no. 7

Link https://doi.org/10.1007/s00145-024-09532-3

2024

Data Redaction in Smart-Contract-Enabled Permissioned Blockchains

Avitabile, G., Botta, V, Friolo, D, Visconti, I, 2024, Data Redaction in Smart-Contract-Enabled Permissioned Blockchains, 6th Distributed Ledger Technologies Workshop (DLT2024)

Link https://ceur-ws.org/Vol-3791/paper9.pdf

2024

Black-Box (and Fast) Non-Malleable Zero Knowledge

Bott, V., Ciampi, M., Orsini, E., Siniscalchi, L., Visconti, I., 2024, Black-Box (and Fast) Non-Malleable Zero Knowledge, Crypto 2024

Link https://doi.org/10.1007/978-3-031-68400-5_14

2023

Privacy and Integrity Threats in Contact Tracing Systems and Their Mitigations

Avitabile, G., Botta, V., Iovino, V., Visconti, I., 2023, Privacy and Integrity Threats in Contact Tracing Systems and Their Mitigations, IEEE Internet Computing, vol. 27, no. 2, pp. 13-19

Link https://ieeexplore.ieee.org/document/9928557

2023

Doubly Adaptive Zero Knowledge Proofs

Botta, V., Visconti, I., 2023, Doubly Adaptive Zero Knowledge Proofs, Theoretical Computer Science, vol. 968, ISSN 0304-3975

Link https://www.sciencedirect.com/science/article/abs/pii/S0304397523003274

2023

Secure Blockchain-Based Supply Chain Management with Verifiable Digital Twins

Botta, V., Fusco, L., Mondelli, A., Visconti, I., 2023, Secure Blockchain-Based Supply Chain Management with Verifiable Digital Twins, ACM Conference on Information Technology for Social Good, ISBN 9798400701160, pp. 291–298

Link https://dl.acm.org/doi/abs/10.1145/3582515.3609547

2023

Extendable Threshold Ring Signatures with Enhanced Anonymity

Avitabile, G., Botta, V., Fiore, D. (2023). Extendable Threshold Ring Signatures with Enhanced Anonymity. Public-Key Cryptography – PKC 2023. LNCS, vol. 13940, pp. 281-311

Link https://link.springer.com/chapter/10.1007/978-3-031-31368-4_11

2022

Efficient Proofs of Knowledge for Threshold Relations

Avitabile, G., Botta, V., Friolo, D., Visconti, I., 2022, Efficient Proofs of Knowledge for Threshold Relations, ESORICS 2022, LNCS 13556, pp. 42-62

Link https://dl.acm.org/doi/10.1007/978-3-031-17143-7_3

2022

Towards Data Redaction in Bitcoin

Botta, V., Iovino, V., Visconti, I., 2022, Towards Data Redaction in Bitcoin, IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 3872-3883

Link https://ieeexplore.ieee.org/document/9917482

2021

Shielded computations in smart contracts overcoming forks

Botta, V., Friolo, D., Venturi, D., Visconti, I. 2021, Shielded computations in smart contracts overcoming forks, Financial Cryptography and Data Security 2021, LNCS 12674, pp. 73-92

Link https://link.springer.com/chapter/10.1007/978-3-662-64322-8_4

2021

Towards Defeating Mass Surveillance and SARS-CoV-2: The Pronto-C2 Fully Decentralized Automatic Contact Tracing System

Avitabile, G., Botta, V., Iovino, V., Visconti, I., 2021, Towards Defeating Mass Surveillance and SARS-CoV-2: The Pronto-C2 Fully Decentralized Automatic Contact Tracing System, Workshop on Secure IT Technologies against COVID-19 (CoronaDef) 2021, ISBN 1-891562-72-X

Link https://dx.doi.org/10.14722/coronadef.2021.23013

PROGETTI

06/2021 – 10/2021

LedgerMPC Toolkit

Ho collaborato all'implementazione del toolkit prodotto dall'Università degli Studi di Salerno per il progetto: https://github.com/danielefriolo/ledgerMPC.

Link https://github.com/danielefriolo/ledgerMPC