CV Andrea Visconti (October 2022)

Andrea Visconti got his Laurea degree (Ms.C. equivalent) and Ph.D. in Computer Science in 2001 and 2005 respectively. Since 2006, Andrea holds a tenured position, Associate Professor (currently) and Assistant Professor (previously), at the University of Milan. He has also been contract professor at University of Trento (Sept 2015 – Sept 2018), member of the Circuit Complexity Team and guest researcher at NIST, United States Department of Commerce (2011 – 2012 and Feb 2012, respectively), and contract professor at University of Insubria (Sept 2005 – Sept 2006). He is also a co-founder of Authclick s.r.l. (Feb 2019 – present), an art-tech startup in Milan.

Andrea is an active researcher in the field of cryptography, security and blockchain technology. He has been involved as Principal Investigator (PI), or co-PI, in the following research projects "Towards fully automatic search of cryptographic trails" (2021, 2 years, PI), "High Speed Cryptography" (2020, 9 months, PI), "Algebraic Analysis of HMAC-SHA-1" (2019, 1 year, PI), "Obiettivo immagine: Estetica della fotografia e cultura del territorio" (2017, 2 years, co-PI), "Analysis of Password-Based Key Derivation Functions" (2015, 3 years, PI), "Optimization of Groebner Basis computations for ECDLP (2017, 9 months, PI)". In 2011 and 2012, Andrea has been a member of Circuit Complexity Team, part of the Cryptographic Technology Group, in the Information Technology Laboratory at NIST, where he worked on the problem of finding "good" – i.e., small, low-depth, few AND gates, and so on – circuits over GF2. In 2002, Andrea was awarded a four years research scholarship at University of Milan on a cryptanalysis project for extracting knowledge from the key space of the asymmetric cryptographic systems via data mining.

His research activities focus on cryptography, coding theory and information security, both theoretical and applied. Past research interests include Biologically-Inspired Computing Systems and Artificial Immune Systems. Andrea is co-author of about 60 papers. He has been keynote speaker of WIDECOM 2021, session chair of ANTIC 2021, technical program co-chair of WIDECOM 2020, general co-chair of the workshop "CRYPTANALYSIS: a key tool in securing and breaking ciphers" (ITASEC 2020), general chair of WIDECOM 2019 and session chair of SECRYPT 2014. Andrea is an Associate Editor of Iran Journal of Computer Science (Springer) and has been member of the program committees of several international conferences and workshops.

Andrea lead a research group of the University of Milan focusing on cryptography, coding theory and information security. He supervised a post-doc, four Ph.D. students and more than one hundred Master/Bachelor students (University of Milan, Trento, Padua, and Milano-Bicocca) to completion of their graduate/undergraduate degree.

In the last decade, he has coordinated and lectured many courses from undergraduate to doctoral students including Cryptography, C Programming Language, Information and Coding Theory, Algorithms and Data Structures, Advanced Programming of Cryptographic Methods, and several Introductory Course of Computer Science.